NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN INVESTIGATION OF WIRELESS SOLUTIONS FOR THE "LAST MILE"

by

Antonios K. Varelas

March 2004

Thesis Advisors: Gilbert M. Lundy
Roberto Cristi

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: An Investigation of Wireless Solutions for the "Last Mile"			**5. FUNDING NUMBERS**
6. AUTHOR(S) Antonios K. Varelas			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The need for broadband network access is experiencing rapid growth, but what is currently available is not sufficient. Copper-based technologies cannot address the requirements of today's bandwidth-intensive Internet applications. End-users in the "last mile" demand access speeds equivalent to those supported by fiber optics backbone networks, although, the cost and time associated with its installation are prohibitive factors for bringing fiber to every home and business. This results in the well-known "last mile access problem," which prevents the Internet from reaching its full potential, and has paved the way for the development of many innovative technologies. Driven by demands for more bandwidth, wireless broadband technologies have been proposed.

This thesis provides an investigation of two candidates to address the lack of adequate bandwidth in the "last mile," *Free Space Optics* (FSO), and the *IEEE 802.11 Wireless Local Area Networking* (WLAN) standard. FSO uses optical signals to deliver information at extremely high data rates, more quickly and cost-effectively than fiber systems. The IEEE 802.11 standard uses radio technology to transfer data. They both use license-free frequency bands for transmission through the atmosphere. They both are quickly deployable, easily scalable, and cheaper than wired solutions, characteristics able to support applications requiring high bandwidth and a high degree of mobility.

14. SUBJECT TERMS Broadband Network Access, Last Mile, FSO, Free Space Optics, WLAN, Wireless Local Area Networking, IEEE 802.11, High Bandwidth, Wireless Broadband Technologies, Fiber Optics			**15. NUMBER OF PAGES** 119
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN INVESTIGATION OF WIRELESS SOLUTIONS FOR THE "LAST MILE"

Antonios K. Varelas
Lieutenant Commander, Hellenic Navy
B.S., Hellenic Naval Academy, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

and

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author: Antonios Varelas

Approved by: Gilbert M. Lundy
Thesis Advisor

Roberto Cristi
Thesis Advisor

Peter J. Denning
Chairman, Department of Computer Science

John P. Powers
Chairman, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The need for broadband network access is experiencing rapid growth, but what is currently available is not sufficient. Copper-based technologies cannot address the requirements of today's bandwidth-intensive Internet applications. End-users in the "last mile" demand access speeds equivalent to those supported by fiber optics backbone networks, although, the cost and time associated with its installation are prohibitive factors for bringing fiber to every home and business. This results in the well-known "last mile access problem," which prevents the Internet from reaching its full potential, and has paved the way for the development of many innovative technologies. Driven by demands for more bandwidth, wireless broadband technologies have been proposed.

This thesis provides an investigation of two candidates to address the lack of adequate bandwidth in the "last mile," *Free Space Optics* (FSO), and the *IEEE 802.11 Wireless Local Area Networking* (WLAN) standard. FSO uses optical signals to deliver information at extremely high data rates, more quickly and cost-effectively than fiber systems. The IEEE 802.11 standard uses radio technology to transfer data. They both use license-free frequency bands for transmission through the atmosphere. They both are quickly deployable, easily scalable, and cheaper than wired solutions, characteristics able to support applications requiring high bandwidth and a high degree of mobility.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author would like to express his sincere thanks and appreciation to his advisors for their assistance, support, guidance and contribution to the completion of this thesis:

Dr. Gilbert M. Lundy

Dr. Roberto Cristi

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Copper wires have brought telecommunication into homes and offices worldwide for several decades, but existing copper and cable infrastructures do not provide sufficient bandwidth for modern applications such as video-on-demand or other high-speed Internet applications. Thus, enormous amounts of capital were invested in building an optical fiber backbone, in order to offer high-speed services. However, most users cannot use these services. They are available for a number of large enterprises and educational institutes, but not for small businesses and houses just one "mile" away from the fiber infrastructure. Homes and offices in the "last mile" need optical fiber bandwidth, but this is not available, since it is not yet economical to deploy new fiber optic cables to every home and business. This situation has resulted in the well-known "last mile access problem." Similarly, there is a strong demand for more bandwidth in military applications, since the availability of high-speed communications is critical for the success of operations that require fast deployment of broadband networks in areas where high-bandwidth infrastructures are not available.

Given the increasing demand for larger bandwidth in both commercial and military applications, the nature of military operations that require a high degree of mobility for achieving the goal of information superiority in the battlefield, and the fact that it is not always and everywhere practical to build and maintain a wired infrastructure, wireless approaches are a promising possibility for providing this bandwidth. Several wireless suggestions have been made, since new wireless broadband technologies are becoming more and more attractive because of their improving performance in terms of bandwidth, cost, simple and fast deployment, and inherent flexibility.

This thesis provides an objective in-depth study of two emerging wireless broadband technologies that have been proposed as potential solutions to the "last mile problem": *Free Space Optics* (FSO) and the *IEEE 802.11 Wireless Local Area Networking* (WLAN) standard. These are explored, discussed and analyzed, both being technologies that offer potential "last mile" solutions. First, the network access problems associated with the existing wired connections in homes and businesses in the "last mile" are dis-

cussed. Then, a study of both FSO and the IEEE 802.11 WLAN standard is provided, by discussing their theoretical background and emphasizing the technological aspects upon which they are based, as well as performance and propagation issues. Next, the thesis identifies and determines their strengths and weaknesses, in general, and as implemented solutions in the "last mile," in particular. This task is accomplished by examining their inherent capabilities and limitations at the technological level, followed by a further investigation of their behavior in practice, under real conditions. This translates to an examination and tracing of the resulting problems, of their operation within different environments that include the most common adverse situations such as unfavorable weather, existence of physical obstructions, presence of interfering sources in proximity, building sway, and security threats. Finally, based on this resolution, the thesis presents a comparison between the two technologies as potential candidates to solve the "last mile problem."

I. INTRODUCTION

The evolution of computing and networking has already changed the world to an incredible degree, and continues to do so day by day. The deployment and establishment of the Internet has had a huge impact on our daily lives. Information delivery is a continuously increasing necessity for more and more people worldwide. However, in addition to deploying appropriate networks, satisfying speeds of data transfers between communicating sites, as well as to and from the Internet, have to be maintained. The demand for broadband network access is experiencing unbelievable growth. Until not many years ago, the maximum processing speeds of chips used in computers was the limiting factor in the development of applications, but this is not the case anymore. Following the evolution of chip technology, computer processing speeds have already reached tremendous rates, and continue to grow, thus constituting less and less an obstacle to high-speed networking [1]. Therefore, the speed constraints associated with the physical media, i.e., twisted pair and coaxial cable, are becoming more and more the issue of concern in today's applications. In addition to the commercial and individual needs for more bandwidth, high-speed communications have always been a very important objective for the military, since the availability of large bandwidth is very critical for military applications, ranging from distance learning to operational applications. The success of the missions conducted by the Armed Forces depends largely on the ability to transfer large amounts of information in a secure, reliable, accurate, and timely way.

Copper wires have brought telecommunication into houses and offices worldwide for several decades, but existing copper wire and cable infrastructures cannot provide the essential bandwidth for the bandwidth-intense applications of our days. In fact, although the media remain the same, the traffic through the existing wires is increasing dramatically. For this reason, large amounts were invested in building the optical fiber backbone, in order to make the offering of high-performance multimedia services feasible. However, in spite of the great demand for these services, most users cannot use them. Connecting to such services has been relatively simple for a number of large enterprises and institutes, but not for small or medium businesses and offices just one "mile" away from the fiber infrastructure, where high-speed Internet is available. Although big companies,

corporations and educational institutes around the world, especially those located in large cities, enjoy high access speeds by using fiber optic cables, the speeds currently available at home are usually lower by at least a factor of ten [2]. Since high-speed Internet is not available for home consumers, developers often hesitate about developing applications capable of offering more advanced services. Thus, applications and services requiring high bandwidth have to wait. Homes and office applications in the “last mile” need the same access speeds that fiber optics provide. However, despite the desperate demand for more bandwidth, the request is usually not satisfied, since it is economically inexpedient to bring fiber optic cables to every house and business there. This situation has resulted in the well-known “last mile access problem.”

The term “last mile” describes the part of the network between the central office, where there is usually a high-transmission line, and the houses and businesses, where the network access speeds are very low [2]. Any telecommunications technology transferring data from the broadband network to and from homes or businesses a short distance away is considered “last mile technology.” The increasing demands for larger bandwidth in both business and residential sectors have led to the development of new wireless broadband technologies that have been proposed as potential solutions to the “last mile problem.”

The cost of deploying new fiber cables to every home and business is more than what most *Internet Service Providers* (ISPs) and clients are willing to pay. Other potential technical solutions to the problem must be able to meet the demands of both the users and the operators. Users desire services convenient to use (always “on”), reliable, and at an affordable cost. Operators want a flexible and scalable technology offering them the capability to continue providing high-quality services when their customer base grows rapidly. Given these circumstances, wireless approaches seem to be the most promising for supporting broadband services in homes and businesses not connected to the fiber backbone. Wireless broadband technologies are becoming more and more attractive because of their better performance in terms of bandwidth, cost, simple and fast deployment, and inherent flexibility (demand-based build out), when compared with the available wired technologies.

In view of the fact that the currently available wired access technologies have proven unable to provide an adequate high-speed solution, several wireless suggestions have been made. This thesis provides an objective in-depth study of two emerging wireless broadband technologies that may be considered a solution to the "last mile problem": *Free Space Optics* (FSO) and the *IEEE 802.11 Wireless Local Area Networking* (WLAN) standard. These will be explored, discussed and analyzed, as both technologies offer high–speed capabilities as potential "last mile" network access options.

The FSO technology is based on transmitting optical signals (invisible beams of light) that carry data from the sender to the desired destination through the atmosphere, instead of fiber optic cables, at extremely high data rates, as well as more cost-effectively and quickly than traditional fiber optic systems [3]. The IEEE 802.11 WLAN standard employs radio technology for transferring large amounts of data over radio waves between the communicating sites, also through the atmosphere. Both technologies use license-free parts of the frequency spectrum for transmission. They both are quickly deployable, easily scalable, and cheaper to install and upgrade in comparison with the wired solutions. These characteristics can support applications that require wide bandwidth and a high degree of mobility. FSO and the IEEE 802.11 WLAN standard are, also, both technologically and economically viable, as evidenced from the numerous new companies that already offer, or will offer in the near future, broadband wireless services. Certainly, both technologies will have a significant impact on the competitive field of broadband telecommunications.

Chapter II identifies the "last mile problem" by analyzing the current broadband connectivity situation in the "last mile," and its related problems.

Chapter III presents a discussion of FSO networking, including a review of its history and evolution, an analysis of the technology upon which it is based, its architecture and implemented topologies. Additionally, factors affecting performance and provided security are also discussed.

Chapter IV provides an analysis of the IEEE 802.11 WLAN standard, including the reasons associated with its use, a review of its birth, development, and dominance in

the wireless market, an extended discussion of the wireless radio technology, in general, and of the IEEE 802.11 family of specifications, in particular, as well as their architecture and services. In addition, performance and security issues are also presented.

Chapter V examines the advantages and limitations of both FSO and the IEEE 802.11 WLAN standard technologies when implemented as “last mile” solutions, and provides a comparison among them in the fields of the greatest interest.

Finally, the conclusions of the above research are summarized in Chapter VI.

II. IDENTIFYING THE "LAST MILE PROBLEM"

A. INTRODUCTION

This chapter discusses and analyzes the issues associated with the use of the currently available wired solutions for providing broadband connectivity to homes and businesses in proximity to the fiber backbone network. In other words, the so-called "last mile problem" will be identified.

B. WHAT IS THE PROBLEM TO BE SOLVED?

In the modern world, the transfer of information is vital to all aspects of daily life such as business, trading, banking, education, and entertainment. In many cases, the instant delivery of critical information is crucial for success. Our Internet world continuously develops and offers new advanced applications and services, but in order to take advantage of its total power, users must have what they want in a fast and reliable way. Demands for high bandwidth, cost-effective, and flexible services on short timelines are increasing at a huge pace in metropolitan networks. This situation has caused a "connectivity bottleneck" [4].

Internet connection speeds are closely related to the existing telephone network, which was not designed for this purpose. Voice communications need much less bandwidth and can tolerate much higher signal degradation than data communications. Telephone calls are handled by the switching system of the *Central Office* (CO), or *Switching Station,* where the copper wires from homes and offices are connected. The central office will either handle a phone call within its own switch, hand it off to another switch in the local area, or transfer it to the long distance network. At the receiving site, the call will be handled by the local central office, before being delivered to its final destination. Multiple switching stations are connected to a *Main Exchange* (ME), and MEs are connected to each other through fiber optics cables. This part of the network is known as the "backbone network." Finally, multiple MEs are connected to an *International Exchange* (IE),

and IEs are interconnected through undersea cables, or satellites, to provide international communications. During the last years, the telephone companies have converted their exchange equipment from analog to digital, which enabled them to offer their customers new services, such as “caller identification,” “call waiting,” answering machine services, touch tone dialing, etc. Most telephone companies are also *Internet Service Providers* (ISPs). Their switching stations are connected to the Internet backbone network with fiber optic cables that support data rates in the gigabit range. Any other ISPs must lease the high-speed fiber connections owned by the telephone companies for accessing the core network. However, in spite of the high data rates supported by the optical fiber cables connecting the switching stations to the rest of the network, the lines between them and the houses are still the old twisted pair copper wires. Consequently, the major part of the “connectivity bottleneck” problem lies between the central office and the houses. This portion of the network, illustrated in Figure 1, is what is called “last mile” [5].

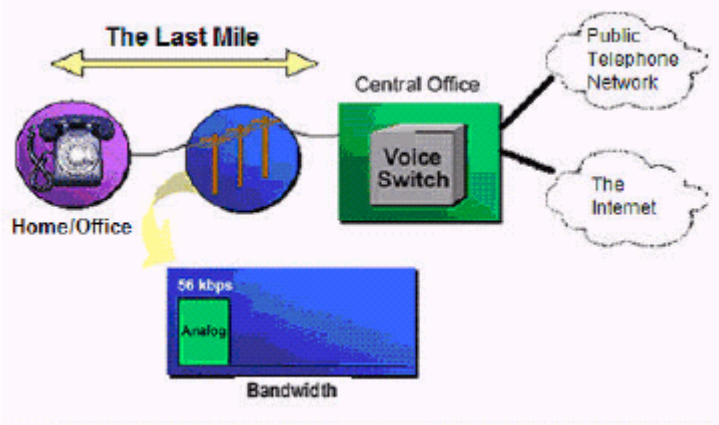

Figure 1. The “Last Mile” Portion of the Telephone Infrastructure [From Ref. 5.]

The telephone network was deployed more than one century ago and its design provided support to analog voice channels with a 4-kHz bandwidth. In the beginning, Internet access from home was performed via very low speed modems. The demand for higher data rates led to the development of new modems able to support speeds up to 56 kbps. To date, due to limitations in quality of the copper wires, length, and encoding

techniques, this is the highest data rate achievable on standard telephone voice lines. These modems are still widely used nowadays. Telephone lines are unshielded twisted pair copper wires, typically several decades old, a fact that often lowers the achievable data rates of 56 kbps dial-up modems well below 50 kbps, even over clean lines [2]. Moreover, the more people attempt to connect, the slower the Internet becomes for everyone, due to the inevitable traffic increase over the telephone lines.

Internet access is not always as slow as it is for the average home user. Broadband access speeds are available at large companies and corporations that consider the investment involved in high-bandwidth connections worthwhile. Nevertheless, these speeds are not feasible for the “last mile” homes, represented graphically in Figure 2, and businesses, where supported data rates are not even close. However, although in most parts of the world Internet access is still mainly performed through 56-kbps dial-up modems, ”semi-broadband” (i.e., data rates up to 2 Mbps) access solutions through the existing infrastructure are already implemented. Most common among them are the *Digital Subscriber Line* (DSL) and cable modems. Copper lines and coaxial cables are the two wired infrastructures available for data transfer to and from the “last mile.” The DSL technology makes use of the twisted pair infrastructure, while cable modems use the same coaxial cable as cable TV, both attempting to provide higher bandwidth to the home users. However, the offered speeds are still limited. There is one more suggested solution based on satellite TV technology, which provides a downstream broadcast link able to send large amounts of information to the home user. The drawback of this alternative is that the upstream capability of a satellite link is very limited, so this solution is not mature yet to be considered an acceptable two-way link for high speed data transfer [2].

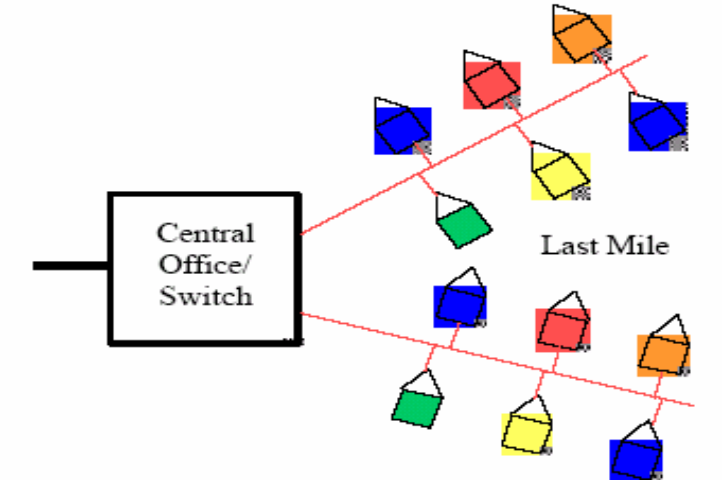

Figure 2. "Last Mile" Homes [From Ref. 2.]

Various higher speed services other than those of dial-up modems are now proposed to home users, but the subscription cost is still high, if these solutions are available at all at the specific area. Many users prefer investing in more computing power, believing that faster processing speeds may improve the situation. However, this is not the problem, as today's personal computers can easily handle the multimedia content that the Internet provides. The problem lies in receiving the tremendous amounts of data. Consequently, the majority of the users that are not willing to pay for higher bandwidth connection are limited by the speed restrictions associated with the use of analog modems. This barrier that blocks the realization of the low-cost high-speed network is at the heart of the "last mile problem."

As previously mentioned, the "last mile" is the part of the telecommunication network starting from the end user's telephone, and ending at the corresponding central office, i.e., the *local loop* connecting a home or office to the local central office. The available bandwidth is only 4 kHz, which limits the transmission of digital data to a data rate of 56 kbps, as discussed earlier. The copper infrastructure is near its maximum capacity, unable to respond to the continuously evolving bandwidth-intensive applications. DSL and cable modems can support data rates up to 2 Mbps, though usually less than 1 Mbps, depending on the distance from the central office and the number of concurrently connected neighbors. However, even the maximum data rate of 2 Mbps is usually not enough when high bandwidth applications are running simultaneously.

Given that the existing infrastructure has reached its practical limits, and both twisted pair lines and coaxial cables face physical restrictions in supporting bandwidth-demanding applications, how can high-speed network access become a reality for homes and businesses in the “last mile”? Why do not just extend the fiber optic cables from the backbone network to the “last mile” homes and offices? Optical fiber is the wired medium that offers the higher bandwidth, but there are several drawbacks involved with a large-scale fiber cable deployment [2]. The major issues are the very high cost and time associated with the digging up of whole neighborhoods (roads, sidewalks, buildings, etc.) for bringing fiber to every house and office. Installing fiber connections to “last mile” residences may cost more than $100 per meter, without taking into account the inevitable maintenance costs [6]. Furthermore, even if fiber lines are deployed, new demands for even higher speeds will soon create the need to upgrade them again, and so on. It should also be underlined that after an investment in fiber deployment has been completed, it becomes a “sunk” cost, since it is impossible to recover. For all these reasons, providers are very hesitant to risk investing in fiber, until the installation and maintenance costs drop significantly. Under these conditions, it is not strange that only 5% of the commercial buildings in the United States are connected to the fiber infrastructure, whereas 75% of them are located just one mile at most from it. Moreover, an average of four additional buildings at a distance of 100 meters correspond to each one of the commercial buildings within the one–mile range from the fiber backbone. It is probable that these businesses employ high–speed LANs, so it would be quite frustrating for them to connect to the outside using lower–speed solutions, such as DSL, cable modems, or T1s [4]. Obviously, if the use of fiber optic cables made sense, the “last mile problem” would be completely solved, and gigabits of data would be a reality in the houses and offices of end users.

Consequently, the “last mile problem” prevents the Internet from reaching its full potential, and affects many people worldwide [6]. The demand for high-bandwidth applications in the “last mile” is increasing every single day, and what is currently available is not sufficient, so the need to solve this problem is bigger than ever. Copper-based technologies (DSL, cable modems, and T1s) cannot constitute a viable solution to the connectivity bottleneck, even though the number of buildings connected via copper lines is much larger than the number of those that enjoy fiber connections. The fact that the

twisted pair infrastructure is widely deployed does not suffice. The problem is bandwidth scalability, and the throughput that copper can support is inherently limited, thus limiting its capability to solve the problem [4]. Fiber is the most appropriate choice to cope with the bandwidth shortage, but the cost and time challenges involved in its installation are prohibitive factors. Optical cables are capable of providing the required bandwidth, but their laying is very time consuming and still too expensive for most users to afford. Given these restrictive parameters, the question then becomes which alternative solutions would have the potential to offer high-bandwidth communications to every "last mile" home or business cost–effectively. This thesis provides an investigation of technical issues related to realizing high–bandwidth data transmission at a reasonable cost. In particular, two wireless proposals, *Free Space Optics* (FSO), and the *IEEE 802.11 Wireless Local Area Networking* (WLAN) standard, are explored as candidates to address the lack of adequate bandwidth in the "last mile."

C. SUMMARY

This chapter analyzed the current broadband connectivity situation in the "last mile" and its related problems.

The next chapter will present an analysis of FSO networking, including its evolution, the technology upon which it is based, and its architecture. Additionally, performance and security issues will be discussed.

III. FREE SPACE OPTICS (FSO)

A. INTRODUCTION

This chapter presents a detailed discussion of the *Free Space Optics* (FSO) technology by providing a review of its evolution, an analysis of the technology itself, implemented topologies, performance and factors affecting it, and security.

B. WHAT IS FSO?

Fiber optics has largely influenced the course of telecommunications worldwide. Fiber optic cables connect telecommunication switches in most countries of the world, but what is missing, as discussed in the previous chapter, are high-speed connections between these switches and the "last mile" [2]. Less than 10% of North America's large buildings are connected to the optical telecommunications network [7]. In the United States, in particular, although the majority of the commercial buildings are within one mile of the fiber optic backbone, they are unable to access it. Only 5% possess fiber optics "to their door" for high-bandwidth services, and the percentages are even smaller in the rest of the world. The connection of buildings with fiber can cost $100,000 to $200,000 per kilometer in metropolitan areas. About 85% of this cost is associated with trenching and installation [8]. Street trenching and digging, apart from being so expensive, also increases air pollution by causing traffic jams, removing trees and, in some cases, even destroying historical sites. Even so, some cities, such as Washington D.C., have thoughts of suspending fiber trenching, while some others, such as San Francisco, are encouraging different carriers to install fiber cables at the same time within the same trench. This situation has resulted because in the past carriers spent large amounts of money to increase the capacity in the core, or backbone, of their networks, but they did not do the same at the network edges. Not surprisingly, this "last mile" became a major bottleneck in any attempt to expand broadband services to many potential customers [8]. Operators are in a difficult position at a time when capital is limited and customers are

demanding high–speed data services. Under these circumstances, a low–cost and simply installed way of overcoming the "last mile" could allow service providers to add customers quickly and easily. However, it should be noted at this point that in some parts of the world the deployment of fiber connections was chosen as the solution to the problem, since there are cases where the availability of high data rates is considered more important than the cost associated with it.

Free Space Optics (FSO), or optical wireless, systems, which can be installed up to a distance of slightly above a mile between each other, could be a viable solution for many applications. FSO is a wireless point–to–point communications technology that offers the possibility of transmitting voice, data, and video based on optical connectivity, but without the need to deploy fiber cables. Information is transmitted through the atmosphere by means of modulated infrared beams. In that way, although in FSO the transmission medium is the air (or free space) instead of fiber or glass, broadband communications offered by fiber optics technology are still possible. The main idea in FSO is using a light source to send a signal through the air, rather than along a glass strand, to a receiver positioned at a close distance. The basis of FSO systems are *transceivers*, i.e., transmitter-receivers, which include one or more laser diode transmitters and a corresponding receiver in a shell, where optical lenses, data processors, fiber connections and an alignment system are also situated [8]. FSO typically uses laser beams, but other types of sources, like *LED*s ("Light Emitting Diodes") and *IRED*s ("InfraRed Emitting Diode") may also be utilized. FSO technology does not depend on any particular protocol and can be used with *Gigabit Ethernet*, *ATM* ("Asynchronous Transfer Mode"), *SONET* ("Synchronous Optical Network") and almost any other network. An example of FSO links appears in Figure 3.

Figure 3. FSO Links [From Ref. 9.]

FSO systems can provide connectivity even over distances of some kilometers, depending mainly on the atmospheric conditions and on the type of light source used. Already available systems in the market can reach capacities up to 2.5 Gbps, while systems offering data rates up to 160 Gbps are under development.

C. FSO HISTORY AND EVOLUTION

FSO is recently becoming popular as a broadband alternative, although the technology has existed for about 40 years, during which most of today's FSO systems engineering has been done, mainly for defense and aerospace applications. These defense applications set the framework upon which today's FSO systems are based [10].

The first attempts to transmit data through the air using lasers were done in the 1960's by scientists who started developing the technology for military applications. The first significant FSO technology advancements began to occur in the United States, Europe and Middle East, where military researchers, engineers and technicians applied the use of infrared lasers in communication devices with the aim of providing secure data and voice transmission that would not be susceptible to the "jamming" of radio frequency–based communication systems. These early FSO systems were capable of transmitting at very low data rates. During the *Cold War*, the development of high–speed and

secure communications was the goal of scientists of both sides. Furthermore, the ability of light to carry information at high speeds over long distances without the severe degradation of the signals attracted the interest of scientists in developing applications for space communication [11]. These laser–based FSO communications had more potential benefits than other wireless technologies, including data rates and security levels beyond those that could be obtained using existing *Radio Frequency* (RF) solutions, but many of the programs did not come to fruition, mainly due to funding cuts.

The development of the first optical fiber for the transmission of data across long distances forced the scientists to reexamine the properties of the optical cable. However, although the research about using optics for transmitting data through the air continued, the industry's interest was more focused on land–based fiber optics [11]. The research on FSO started again in the early 1990's, and the technology was mostly viewed as a broadband alternative. FSO applications also started to be examined as possible fast and affordable solutions for providing high–speed access to buildings not connected with fiber cables, without having to dig trenches for installing them.

D. HOW FSO WORKS

FSO uses the *InfraRed* (IR) range of the electromagnetic spectrum, which can be seen in Table 1. The wavelengths used by FSO systems are close (slightly smaller) to those of visible light. FSO networks are based on either 780-to-850 nm or 1,550 nm laser wavelength systems, corresponding to frequencies from 194 THz for the 1,550 nm wavelength and up to 385 THz for the 780 nm wavelength. These specific wavelengths fall into two spectral regions that do not suffer significant *absorption* due to the local atmospheric conditions. Since these wavelengths are also used in fiber-optic communications, industry standard components can be used on both the transmission and receive sides. Due to the proximity to the *visible spectrum*, the wavelengths in the *near IR spectrum* have nearly the same propagation properties as visible light.

	Frequency	Wavelength
ELF	3Hz to 30Hz	100'000km to 10'000 km
SLF	30Hz to 300Hz	10'000km to 1'000km
ULF	300Hz to 3000Hz	1'000km to 100km
VLF	3kHz to 30kHz	100km to 10km
LF	30kHz to 300kHz	10km to 1km
MF	300kHz to 3000kHz	1km to 100m
HF	3MHz to 30MHz	100m to 10m
VHF	30MHz to 300MHz	10m to 1m
UHF	300MHz to 3000MHz	1m to 10cm
SHF	3GHz to 30GHz	10cm to 1cm
EHF	30GHz to 300GHz	1cm to 1mm
Infrared	300 GHz to 400 THz	1mm to 770nm
Visible Light	400THz to 900THz	770nm to 330nm

Table 1. The Electromagnetic Spectrum [From Ref. 12.]

The two operating ranges of wavelengths differ in power requirements, achievable distances, and attainable data rates. Consequently, there are also differences in their cost. The 1550-nm systems allow the safe use of lasers of much higher power, compared to those used in the 780-to-850 nm systems. This results from the fact that wavelengths of less than 1400 nm may cause damage to the human eye, since they are focused by the cornea into a concentrated spot falling on the retina [13]. Since operating at 1550 nm is safer for the eye, lasers are allowed to operate at higher power in that part of the spectrum, and this makes it easier to produce transmitters that can deliver enough power over longer distances. Thus, the 1550-nm laser is better in terms of power, distance, and data rates. More precisely, it typically uses about two orders of magnitude higher power than the 850 nm laser. The link lengths can be increased by a factor of at least five because of this increase in power and, at the same time, sufficient signal strength for proper link operation is maintained. Alternatively, it is able to provide higher data rates over links of the same length. Therefore, the 1550-nm wavelength enables much greater power to travel over longer distances or at higher data rates, so it seems preferable for long distances, high data rates, poor propagation conditions, or combination of these. However,

the equipment cost is significantly higher. The 850-nm wavelength systems cost about ten times less than the 1550-nm wavelength ones to manufacture. The cost of a 1550-nm laser offering data rates of gigabits per second over a few kilometers is about 50,000 dollars, whereas the cost of an 850-nm laser with attainable data rates of around 10 Mbps over a few hundred yards costs approximately 5,000 dollars [14]. There are, nevertheless, applications associated with both wavelengths and there is room for both in the market. There may be applications that need only the smaller, and cheaper, bandwidth, while some others may require higher power or larger bandwidth over greater distances.

The clear *line–of–sight* between the source and the destination is required. If a line–of–sight is available, strategically positioned mirrors may be used to reflect the energy [5]. In a basic *point–to–point* transmission system, an FSO transceiver ("link head") is placed on either side of the transmission path. Transceivers may be mounted on rooftops, on building corners, or behind windows, as illustrated in Figure 4. The beams can pass through glass windows with low or no attenuation as long as the windows are clean. The maximum distances between transceivers depend on the local weather conditions, ranging from about 600 feet to a mile in a clear and dry atmosphere [13].

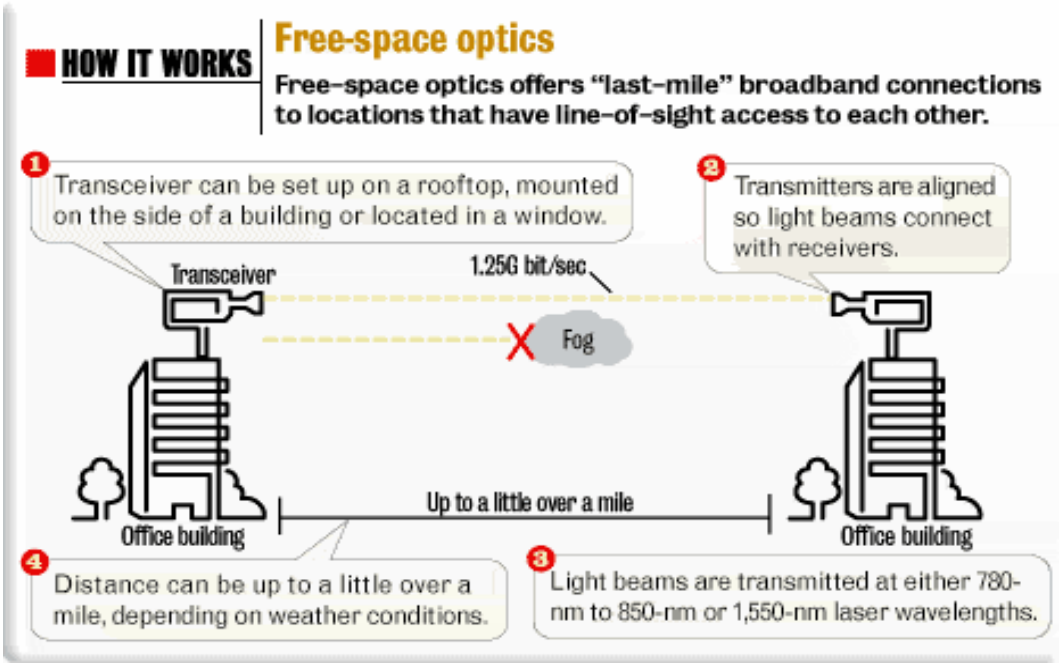

Figure 4. A Point–to–Point Transmission Path [From Ref. 13.]

The optical transceiver consists of a laser transmitter and a detector to provide full duplex capability. Figure 5 displays a *LightPointe Communications Inc.*'s laser node. The data to be transmitted modulates the beam at the source, while a photodetector receives the beam at the destination and the data is "demodulated" from the beam. The resulting signal is then amplified and sent to the hardware [5].

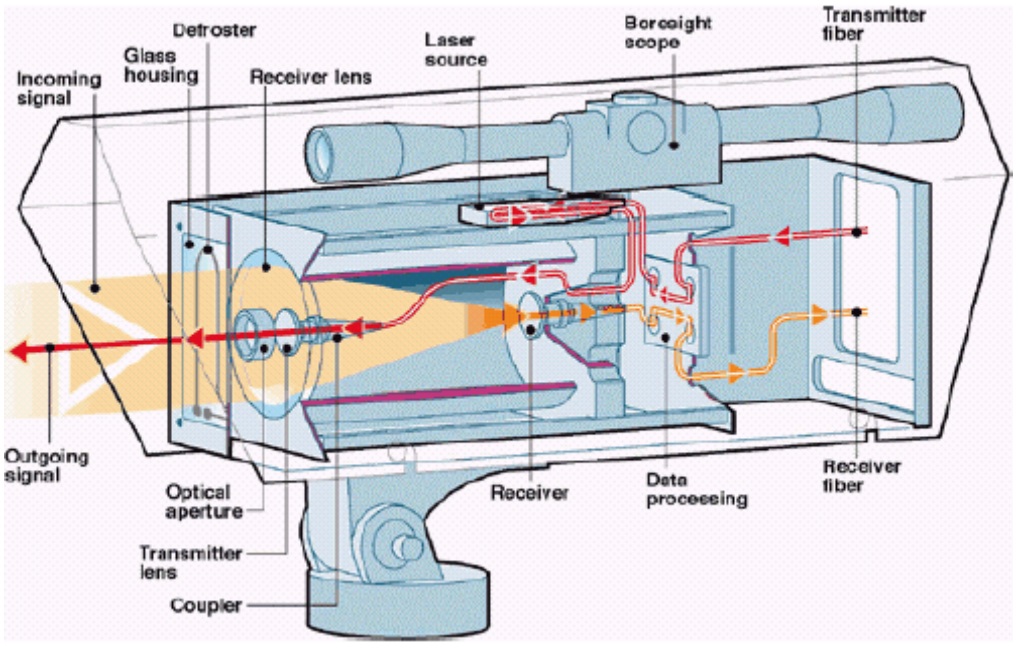

Figure 5. LightPointe Communications Inc. Node [From Ref. 14.]

A light source and a telescope assembly form the optical part of the laser transmitter. The telescope may use either lenses or a parabolic mirror, and its task is narrowing the laser beam and projecting it to the receiver. The transmission beam's divergence may range from a few hundred microradians up to a few milliradians. In FSO equipment of moderate range, there is a divergence of one milliradian, resulting in a beam diameter of one meter at a distance of one kilometer. A lens, or a mirror, is used at the receiver for picking the transmitted light, which is then focused on a photo detector. As seen in Figure 6, the receiving telescope is much smaller than the projected beam, whose diameter, depending on the actual beam divergence, can be several meters, compared to an 8-20 cm diameter of a typical telescope. In view of this fact, a significant portion of the transmit-

ted light is lost during the transmission, a phenomenon called “geometrical path loss”. This loss can be reduced by using narrower laser beams, but this requires increased stability of the mounting platform, or more advanced *active beam-tracking* systems [6].

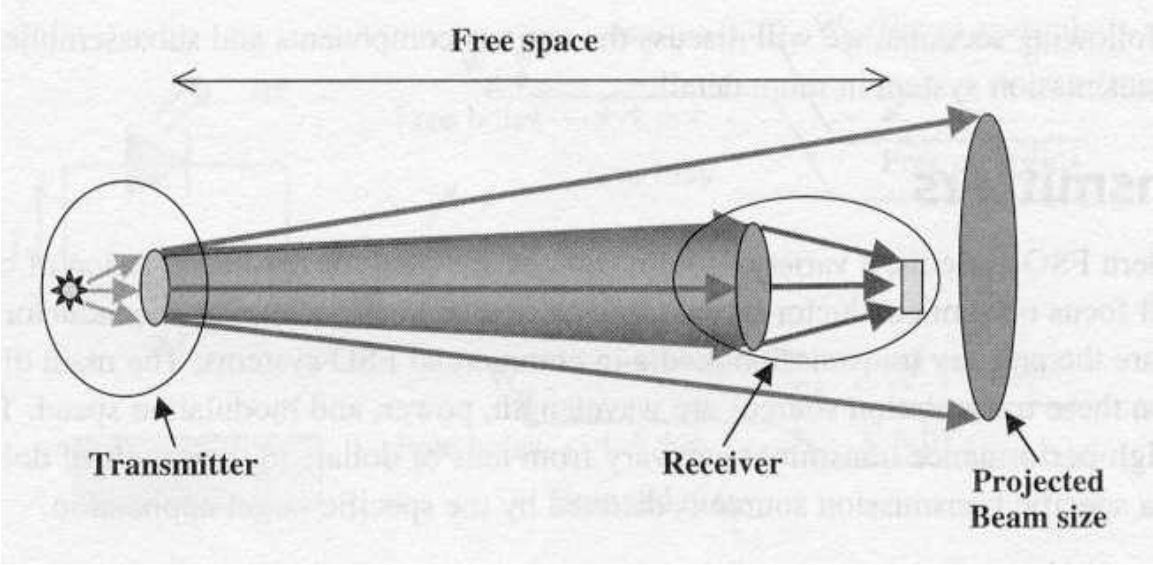

Figure 6. A Free-Space Optical Transmission System [From Ref. 6.]

In FSO systems, data may be transmitted and received at the same time, i.e., the operation of FSO transceivers is *full duplex*. The data to be transmitted is converted from the electrical domain into the optical one, during an electro-optic conversion process that makes the network’s transportation protocol transparent to the transmission path. In this manner, the transmission of information between two networking locations is performed at the *physical layer*. After the modulated light signal has been collected by the receiver’s telescope, the optical signal is converted back to an electrical signal [6].

In accordance with the above, the main components of a FSO system are a light source, optics to direct and focus it, and a receiver that, apart from receiving abilities, includes electronics for electro–optic conversions. These requirements are similar to those of the conventional fiber optics technology, apart from some particularities originating from the use of the free space as the transmission medium, instead of fiber cables [6].

A number of factors impact the selection of a laser source. The main requirement is that the wavelength used by the source in the transmission must be correlated with one of the adequate atmospheric windows, which are around 850 nm and 1550 nm. In addition, the selection of a particular laser source should also consider the power of transmission, the lifetime, the cost and availability of commercial products, the dimensions, the compatibility with other transmission media, such as fiber, the modulation capabilities, as well as eye safety issues. The selection of a light detector is based on the specific application, since the decision of which material to use depends on the transmission wavelength in the light source [6].

E. FSO TOPOLOGIES

Possible topologies for "last mile" networks are characterized by their level of flexibility, scalability, and supported redundancy. FSO systems offer the flexibility to be deployed in numerous architectures. Indeed, several network topologies can be employed in FSO networks. The most important among them are *point–to–point*, *point–to–multipoint* (or *multipoint–to–point*, or *star*), *point–to–consecutive point* (or *ring*), and *mesh* architectures [15].

1. Point–to–Point

It is the simplest topology for connecting network nodes, since data travels over a single, uninterrupted, and dedicated path between two nodes, as seen in Figure 7. Point–to–point FSO connections provide higher bandwidth, but they are less scalable. However, with the use of FSO point–to–point links, buildings not connected, but near to the optical fiber backbone network, can be connected to it very quickly and economically.

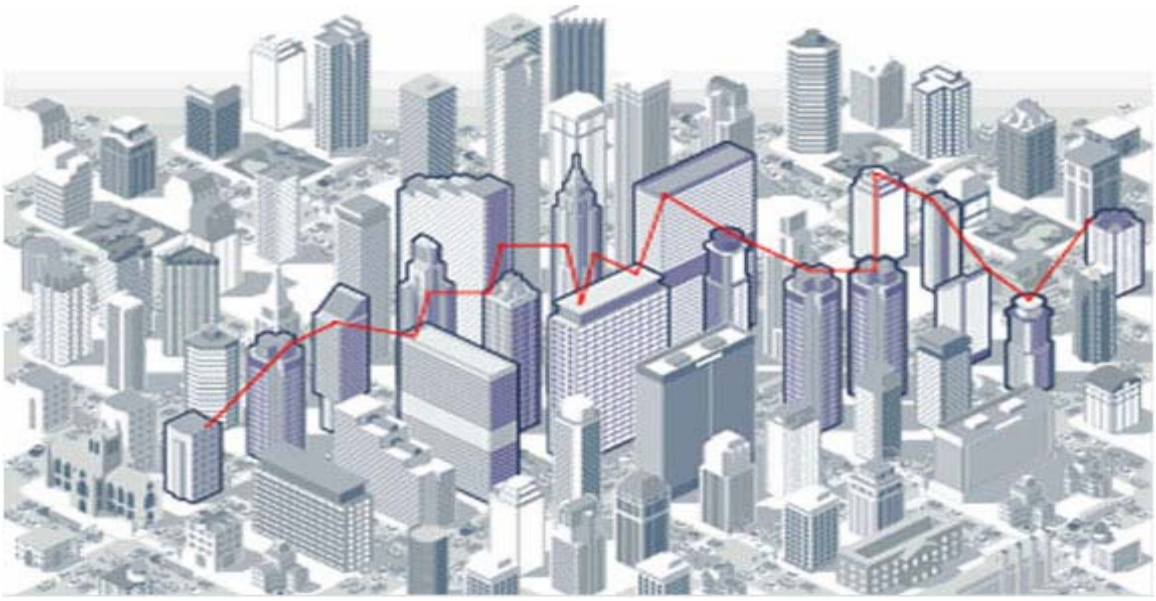

Figure 7. A Point–to–Point Topology [From Ref. 9.]

2. Point–to–Multipoint or Multipoint–to–Point (Star)

Every node is connected to a central node via independent FSO links, as illustrated in Figure 8. The central node is usually a *hub* or a *multiplexer* that forwards data through the use of *repeaters*. The topology is based on the *cell concept*, where each cell is associated with a *base station* that links remote users in a shared–environment situation. The point–to–multipoint architecture offers a wide range of easily installable options, since it can also be deployed from roof to roof, from window to roof, and from window to window. Additionally, the topology offers cheaper connections and easy scalability through node addition. However, these features limit the available bandwidth, comparing it to the point–to–point option.

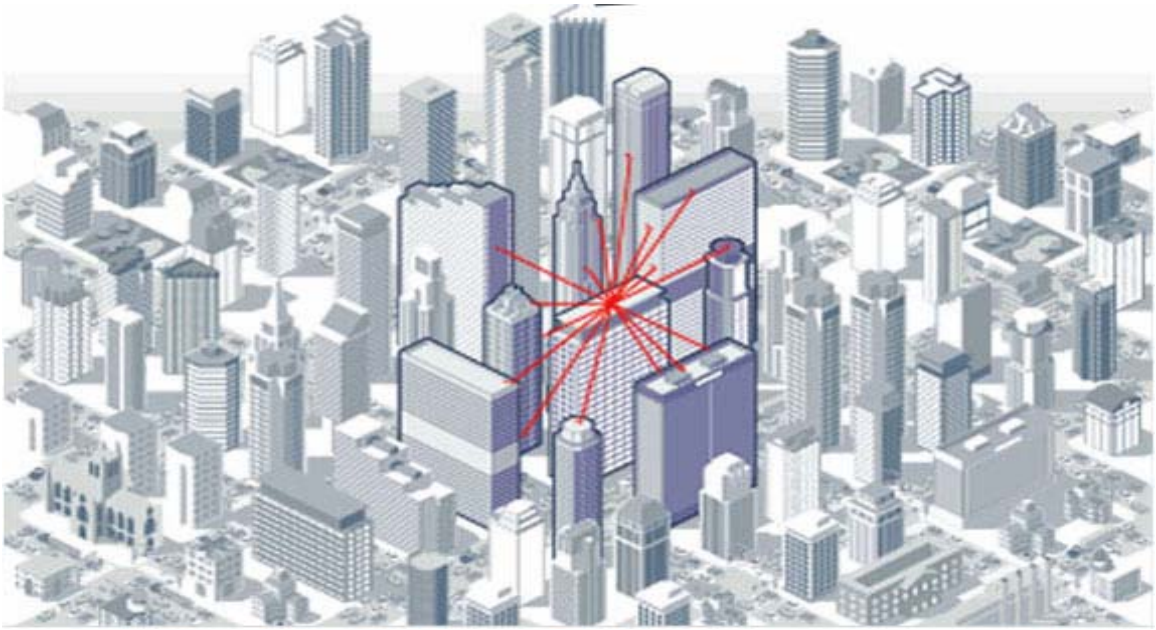

Figure 8. A Point–to–Multipoint Topology [From Ref. 9.]

3. Point–to–Consecutive–Point (Ring)

In this topology, each node is directly connected to one node on each side of it, in such a way that all nodes together form a loop. Thus, a ring topology consists of multiple nodes and point–to–consecutive–point FSO links deployed in closed loops, as in Figure 9. This type of architecture is not easily scalable, but it offers a high level of survivability by transmitting the same data along different directions. In order to address the issue of a single point of failure, links connecting multiple buildings in a ring configuration can be combined with point–to–point or point–to–multipoint links to provide redundancy in a selective way when customers desire this. Consequently, the ring topology is a robust and scalable network architecture.

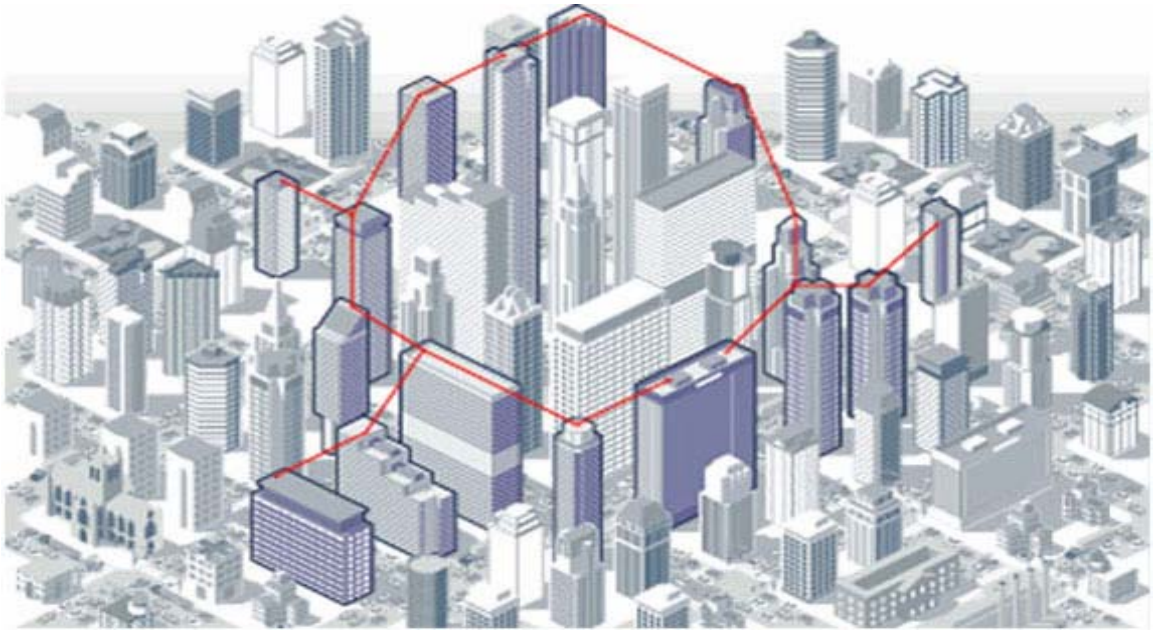

Figure 9. A Ring Topology [From Ref. 9.]

Figure 10 summarizes all the topologies mentioned above.

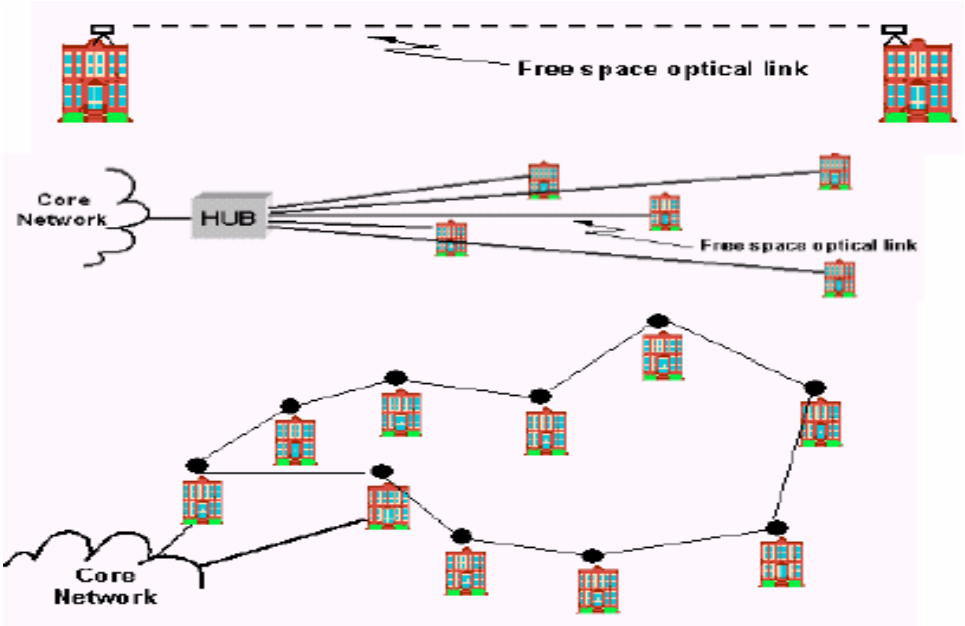

Figure 10. The Point–to–Point, Star and Ring Topologies [From Ref. 16.]

4. Mesh

A mesh topology consists of nodes connected by many redundant FSO connections, as shown in Figures 11 and 12, which construct a partial or full mesh network. The presence of multiple redundant links provides protection against multiple points of failure. However, environmental conditions may cause the simultaneous failure of adjacent links. Moreover, the mesh architecture constrains the allowable links' lengths more than the other solutions. Although these disadvantages limit the cost/benefit advantages and usefulness of a FSO mesh network in comparison to a conventional fiber mesh network, higher reliability due to the redundant connections, and easy node addition are quite important features. In addition to reliability and scalability, mesh topologies constitute an attractive solution for "last mile" access because they also do not require excess bandwidth for duplicating the data traffic. Although most mesh topologies are based on the ATM protocol, "last mile" networks employ more and more the Ethernet protocol, which integrates with end–user networks without high traffic overhead, guarantees quality of service for real–time and critical applications, and simplifies traffic–engineering control.

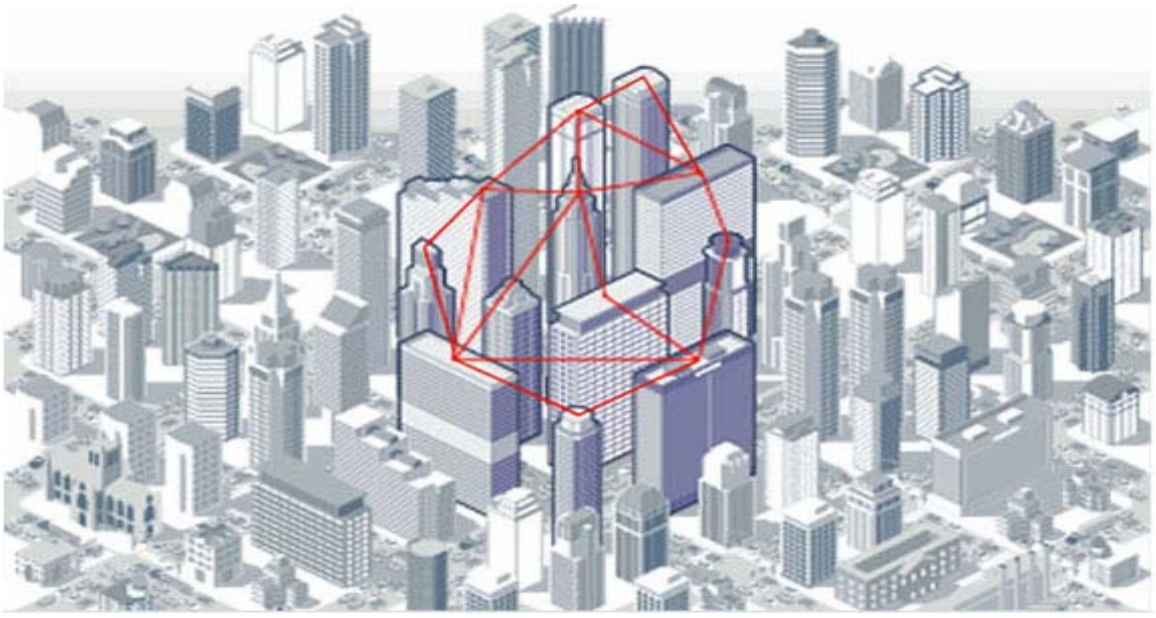

Figure 11. A Mesh Topology [From Ref. 9.]

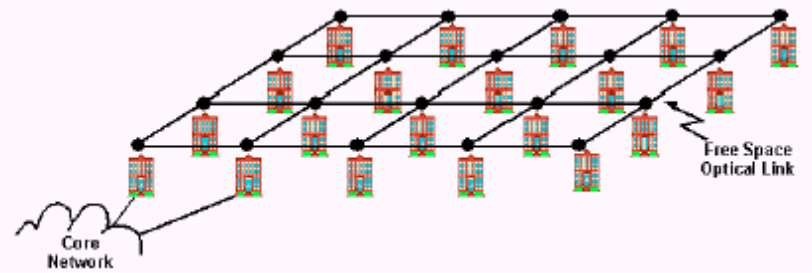

Figure 12. Typical Mesh Configuration for FSO Systems [From Ref. 2.]

All the above topologies actually are a combination of point–to–point links. Furthermore, FSO networks can be deployed using *hybrid* topologies that include ring, point–to–point and/or star interconnections. In ring interconnections, nodes themselves may be rings, whereas point–to–point links with nodes not belonging to rings can still exist. In star interconnections, central nodes are connected with other central nodes via point–to–point links. The extension of standard network topologies allows the coverage of wider areas at low cost, while it yields higher network reliability [16].

F. FACTORS AFFECTING FSO PERFORMANCE

In a FSO system link, the atmosphere causes signal degradation and attenuation in several ways, including *absorption*, *scattering* (mainly *Mie scattering*), and *scintillation*. These effects contribute to channel fade and depend on the current local conditions and weather, so they are time varying. Even a clean, clear atmosphere is composed of oxygen and nitrogen molecules, whereas the weather can contribute large amounts of water vapor. Other constituents can exist, as well, especially in polluted regions, and these particles may absorb or scatter infrared photons that propagate in the atmosphere [17].

The design of FSO networks has to take into account the unpredictable nature of the earth's atmosphere, in order to face its effects on the performance of FSO systems. The final goal of a link budget calculation is to determine the distance that the transmitter and the receiver can be placed apart, while there is still enough margin left to allow for a specified minimum link availability. After having chosen a distance, the link fade margin corresponding at this distance is calculated, and this value can serve as a measurement of

the link's reliability. Moreover, it is possible to take advantage of the optimal atmospheric windows, if suitable wavelengths are chosen for the transmission. Therefore, FSO systems operate in atmospheric windows in the near infrared spectral windows located around 850 nm and 1550 nm, in order to ensure a minimum amount of signal attenuation from scattering and absorption [17]. Figure 13 shows the absorption of different atmospheric gases in relation with different wavelengths. The first graph illustrates the absorption of *methane*, the second graph the absorption of *nitrous oxide*, the third graph the absorption of *oxygen* and *ozone*, the fourth graph the absorption of *carbon dioxide*, and the fifth one the absorption of water, whereas the sixth graph illustrates the composite absorption of all the above gases, so this is actually the absorption of the atmosphere. It can be observed that *ultraviolet light* wavelengths (below 0.3 μm) are largely absorbed by oxygen and ozone, *visible light* wavelengths (0.4 to 0.7 μm) are slightly absorbed by oxygen and ozone, the *near infrared* wavelengths (0.7 to 1.5 μm), commonly used in FSO, are largely absorbed by water molecules at several wavelengths, and *infrared* wavelengths above 1.5 μm are absorbed by all gases at different degrees, depending on the particular wavelength [18].

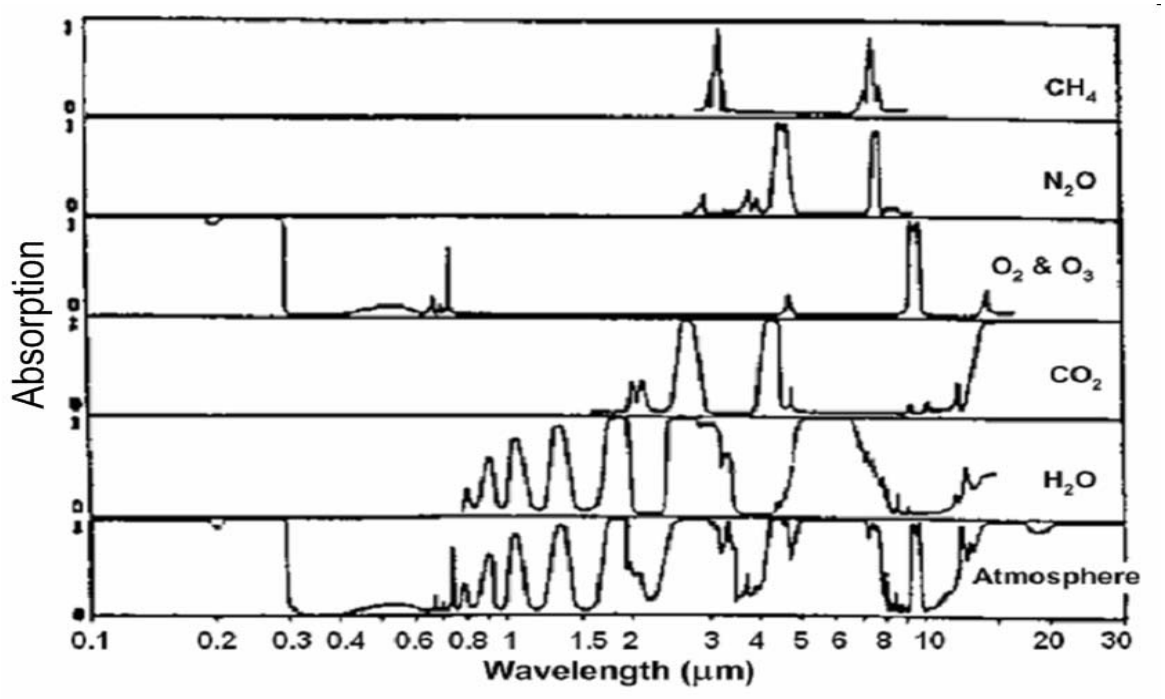

Figure 13. Atmospheric Transmittance [From Ref. 18.]

Another significant issue to consider in the deployment of FSO networks is that buildings naturally move and sway, due to winds, or even seismic activity. Building movements affect beam aiming that, in case of mispointing between the receiver and the transmitter, can result in signal interruption or loss [16].

Finally, potential violations of the line–of–sight requirement will have an adverse impact on the operation of FSO systems. Due to the narrow beam and the high data rates, not only solid obstacles, like buildings or trees, but small objects may also influence FSO communications. Even various flying objects such as birds passing through the optical path can affect a FSO link, because they may block the line–of–sight between a transmitter and a receiver, causing the interruption of the communication. This is not a major issue in mesh architectures thanks to redundant links.

The above factors that can possibly affect the performance of a FSO system are analyzed below:

1. Atmospheric Attenuation Theory

a. Scattering

Scattering is caused when a ray of light collides with various molecules found in the atmosphere. The physical size of these molecules determines the type of scattering. When it is smaller than the wavelength, a *Rayleigh scattering* takes place [19]. More specifically, Rayleigh scattering results from particles of size less than approximately one-tenth of the used wavelength's size and mainly consists of scattering off the surfaces of particles in the air. Rayleigh scattering highly depends on the selected wavelength [20]. When the particles' sizes are comparable or are larger than the wavelength, this is called "Mie scattering." Consequently, in the near infrared wavelength range, fog, haze and pollution (aerosols) particles are the major contributors to the Mie scattering process [17]. Mie scattering does not depend on wavelength size as much as Rayleigh scattering does. When particles have sizes much larger than the wavelength, it is known

as “non-selective scattering”. In scattering, only a directional redistribution of energy takes place, and not a loss of energy, as happens in absorption, but this energy redistribution can result in a significant reduction of the beam intensity in the case of longer distances.

Figure 14 illustrates the physics of the light scattering mechanism while the light beam travels from the originating laser source to the receiver.

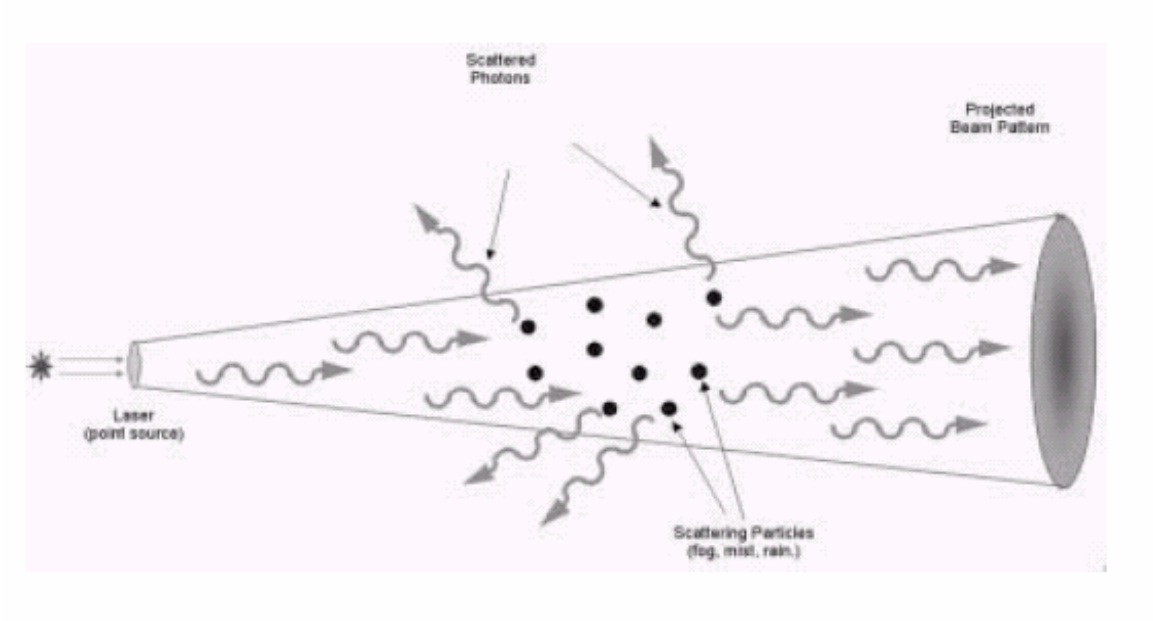

Figure 14. The Light Scattering Mechanism [From Ref. 21.]

b. Absorption

Absorption is a phenomenon taking place when suspended molecules from different gases in the atmosphere extinguish photons. The resulting effect in FSO systems is the attenuation (power decrease) of the laser beam, which directly affects the availability of a system. The degree of absorption differs from one transmission wavelength to another. Nevertheless, by using the appropriate power, based on the particular atmospheric conditions, as well as *spatial diversity* (multiple beams within an FSO unit), the required level of network availability can be maintained [19].

c. Turbulence

In hot areas, when the ground heats up on a sunny day, the air heats up, as well, and some air cells or air "pockets," heat up more than others. These temperature variations among the various air pockets, created by heated air rising from the ground, or even various operating devices, provoke changes in the *refraction index*, which in turn, changes the propagation path of the light through the air. These air pockets are not stable in space and in time, so the change of the refraction index seems to follow a random motion that appears as turbulent behavior [17]. Since the laser beam is affected by the refraction, turbulence might cause pointing errors, while it may also cause *fading*, as explained below. The effects experienced by laser beams because of turbulence are as follows.

(1) Beam Wander. This is the phenomenon of an optical beam wandering in the atmosphere and is caused by the random deflection of the beam through the changing refractive index cells, as Figure 15 illustrates. The light will be focused or defocused randomly, following the index changes of the transmission path, since refraction through a medium, such as air, bends the light in the same way as light passing through a refractive medium such as glass [17].

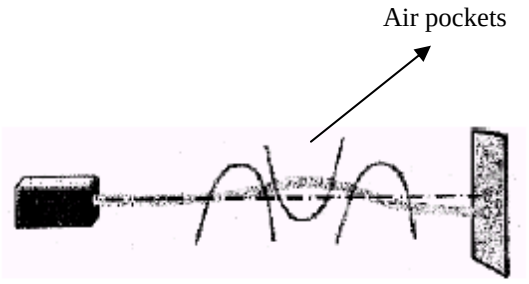

Figure 15. Beam Wandering [After Ref. 22.]

(2) Beam Spreading. As an optical beam propagates through the atmosphere, it spreads up to a certain degree. This spread of the beam may be more ex-

tended than diffraction theory predicts. The spot size can often reach twice the size of the diffraction-limited beam diameter. Many FSO systems incur approximately one meter of beam spread per kilometer of distance [17].

(3) Scintillation. One result of turbulence is the variation in the spatial intensity distribution of the laser beam [22]. The resulting distortion of the beam's wave front, which may cause fluctuations in the signal's amplitude, is known as "scintillation." Constructive and destructive interferences, due to variations in the arrival times, lead to "image dancing" at the receiver end [15] (see Figure 16). Of the three turbulence effects, this is the one that might most affect FSO systems. Strong scintillations may cause signal fading, i.e., signal power decreases below a threshold value, which leads to bit errors. In order to minimize the effects of scintillation on the transmission path, FSO systems should not be installed close to hot surfaces. In view of the fact that scintillation decreases with altitude, FSO systems should be installed slightly above the rooftop at more than four feet. For the same reason, the beam path must be more than five meters above city streets or other potential sources of severe scintillation [17].

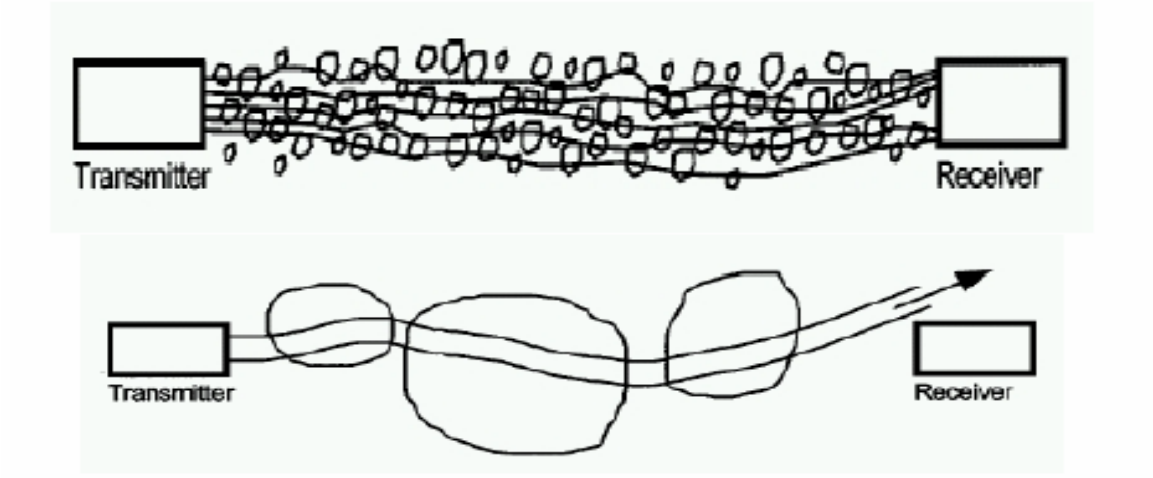

Figure 16. Scintillation [From Ref. 22.]

2. The Impact of Weather

Interference due to the weather, especially fog, is the primary limitation to the performance of FSO systems. The weather's type and intensity determines its impact on FSO networks. Rain and snow create problems only under severe conditions, but fog might significantly aggravate the attenuation of the signal. Interference due to fog in optical transmission is similar to fading because of rain in radio transmissions, a well-known phenomenon. Fading results from the scattering of the beam in the atmosphere, as it encounters various particles, and it is a combination of two main processes, Rayleigh and Mie scattering. Rayleigh scattering due to rain barely affects FSO wavelengths, even though it is the main process causing signal fading to radio wavelengths [20]. On the contrary, Mie scattering is the dominant process responsible for fog interference at FSO communications.

a. Rain

Despite the fact that its impact is significantly less than that of fog, rain still has a distance–reducing impact on FSO. Nevertheless, the maximum attenuation is 20 dB/km, even in the heaviest rain (cloudbursts of 100 mm/hr) [23]. The reason is that raindrops have radii much larger (200-2000 μm) than the wavelengths of FSO signals, which, being on the order of 1 μm, are too short to be significantly affected by Rayleigh scattering [20]. On the other hand, RF wireless technologies that use frequencies above approximately 10 GHz are significantly affected by rain and little affected by fog. The reason is that RF wavelengths are much closer to the radius of raindrops, and both are larger than the moisture droplets of which the fog is composed [17]. Thus, radio signals, especially high-frequency ones, which have wavelengths in the millimeter to centimeter range, are susceptible to rain fading by Rayleigh scattering [20]. At this point, it should be noted that the lower RF frequencies in the 2.4-GHz and 5-GHz ranges, which do not

require licenses, are relatively unaffected by rain and fog, but this lack of licensing means more potential users and, hence, possible severe interference probability at the 2.4-GHz band, which was chosen for the operation of several commonly used devices.

Rain is characterized by moderate attenuation values. A rainfall of 2.5 cm/hour, for example, causes a signal attenuation of 6 dB/km. Therefore, FSO systems which operate with a 25-dB link margin can penetrate rain relatively unimpeded, especially when systems are deployed in metropolitan areas where buildings distances are usually much less than one kilometer. If, for example, the system is deployed over a distance of 500 meters under the same rain conditions, the attenuation is only 3 dB/km. However, if the rain rate increases above the cloudburst level (more than 10 cm/hour), the resulting attenuation may be a problem in deployments beyond the typical metropolitan distances, but the cloudbursts usually last for only a short period of time [17].

b. Snow

Snow is composed of ice crystals having various shapes and sizes, but in general, snow is larger than rain. Snowing conditions can attenuate the beam, but scattering is not a significant issue for FSO systems, since the size of snowflakes is larger than the operating wavelength. The impact of light snow to blizzard and whiteout conditions is approximately between light rain and moderate fog, with link attenuation values from 3 dB/km to 30 dB/km [17].

c. Fog

Fog is considered as the biggest challenge for FSO communications. As explained above, rain and snow do not seriously affect FSO systems, but the impact of fog is much more important. Fog is composed of water droplets having a radius in the same order with the size of near infrared wavelengths, which is the reason why fog is the most hurtful weather phenomenon to FSO. In fact, through a combination of absorption, scattering and reflection, fog can alter the characteristics of light, or even completely ob-

struct the passage of it [19]. The main loss mechanism for fog is scattering. As previously mentioned, fog interference at the operational wavelengths of FSO systems is due to the Mie scattering process. It is interesting to note that fog and clouds appear white because of Mie scattering, since all the wavelengths of the visible light are scattered in an equal manner by the moisture particles of clouds. FSO signals are scattered by fog in a similar way, because their wavelengths are close to the wavelength of visible light. These wavelengths are very small, compared to the raindrops size, so they pass through rain lightly affected. By contrast, their size is close to the size of water droplets in fog, ranging from 10 to 50 μm . Therefore, they are largely scattered by Mie scattering [20]. This impact of fog on FSO communications is exactly analogous to the effect of rainfall on RF wireless communications, which leads to fading and attenuation.

The signal reduction due to atmospheric attenuation loss can vary from 0.2 dB/km in very clear weather, up to about 350 dB/km in very heavy fog (compared to single–mode fibers that attenuate at 0.5 to 0.2 dB/km and to current multimode fiber-optic cables that attenuate at 2 to 3 dB/km). The availability of an FSO system can be reduced by the large attenuation values provoked by heavy fog [23].

Typically, in fog, the visibility ranges between 0 – 2,000 meters. When the visibility is more than 2,000 meters, the weather condition is usually referred to as “hazy”. Since it is difficult to describe the appearance of fog by physical means, often expressions such “thin fog” or “dense fog” are used to characterize the various foggy conditions. Different degrees of fog are characterized by different distribution of the particle sizes, but even modest fog conditions can highly attenuate infrared signals over shorter distances [17].

In order to address fog, the transmission power must be maximized, up to the limits of eye safety. Link lengths have to be designed for a specified availability level, considering the local weather statistics for fog, and network redundancies must be added. New laser transmitters are now dealing with fog interference, the most important of the handicaps that have prevented the wide acceptance of FSO technology. Laser diodes with

high-performance micro-optics can be used to optimize the output beam quality for greater fog–penetrating power, resulting in a beam with significantly improved fog–penetrating ability [20].

The impact of the weather on FSO systems, as far as losses and achieved distances are concerned, is shown in Table 2, where different weather conditions are associated with their visibilities, and the corresponding attenuations and link distances.

Weather condition	Precipitation	mm/hr	Visibility	dB loss/ km	TerraLink 8-155 Range
Dense fog			0 m		
			50 m	-315.0	140 m
Thick fog			200 m	-75.3	460 m
Moderate fog			500 m	-28.9	980 m
Light fog	Cloudburst	100	770 m	-18.3	1.38 km
			1 km	-13.8	1.68 km
Thin fog	Heavy rain	25	1.9 km	-6.9	2.39 km
			2 km	-6.6	2.79 km
Haze	Medium rain	12.5	2.8 km	-4.6	3.50 km
			4 km	-3.1	4.38 km
Light Haze	Light rain	2.5	5.9 km	-2.0	5.44 km
			10 km	-1.1	6.89 km
Clear	Drizzle	0.25	18.1 km	-0.6	8.00 km
			20 km	-0.54	8.22 km
Very Clear			23 km	-0.47	8.33 km
			50 km	-0.19	9.15 km

Snow

Table 2. Impact of Weather on a FSO System [From Ref. 5.]

3. Addressing Building Movements – Tracking and Acquisition

Theoretically, in an electromagnetic transmission, the waves in the source are related with a constant phase relationship and travel directly to the receiver, which means that only one single frequency is required for transmitting data. This can be achieved with

a fully coherent source, as illustrated in Figure 17, which is an unrealistic situation. In practice, the light source must transmit a very small range of frequencies, using an equivalently narrow bandwidth. Moreover, even then the waves in the source interfere with each other, resulting in the divergence of the beams (see Figure 18). If this divergence is less than the sway of the building where the transmitter is mounted, a beam traveling to the receiver may be totally mispointed, and, thus, miss its target. In order to avoid this potential, at least half of the laser beam must reach the receiver. Accordingly, a beam's divergence has to be at least two times larger than the angle of the expected building's sway, as shown in Figure 19 [18].

Figure 17. Coherent Electromagnetic Transmission [From Ref. 18.]

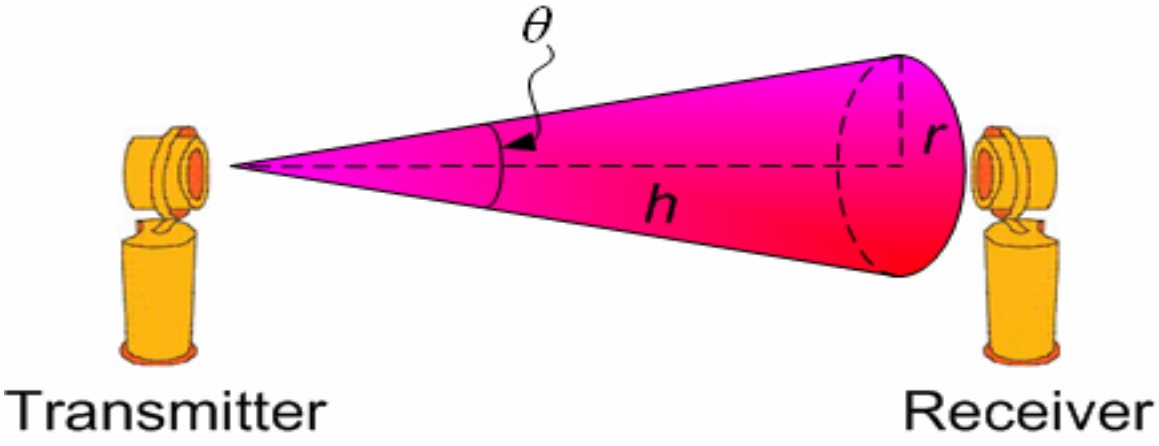

Figure 18. Beam Divergence Resulting from Non-Coherent Electromagnetic Transmission [From Ref. 18.]

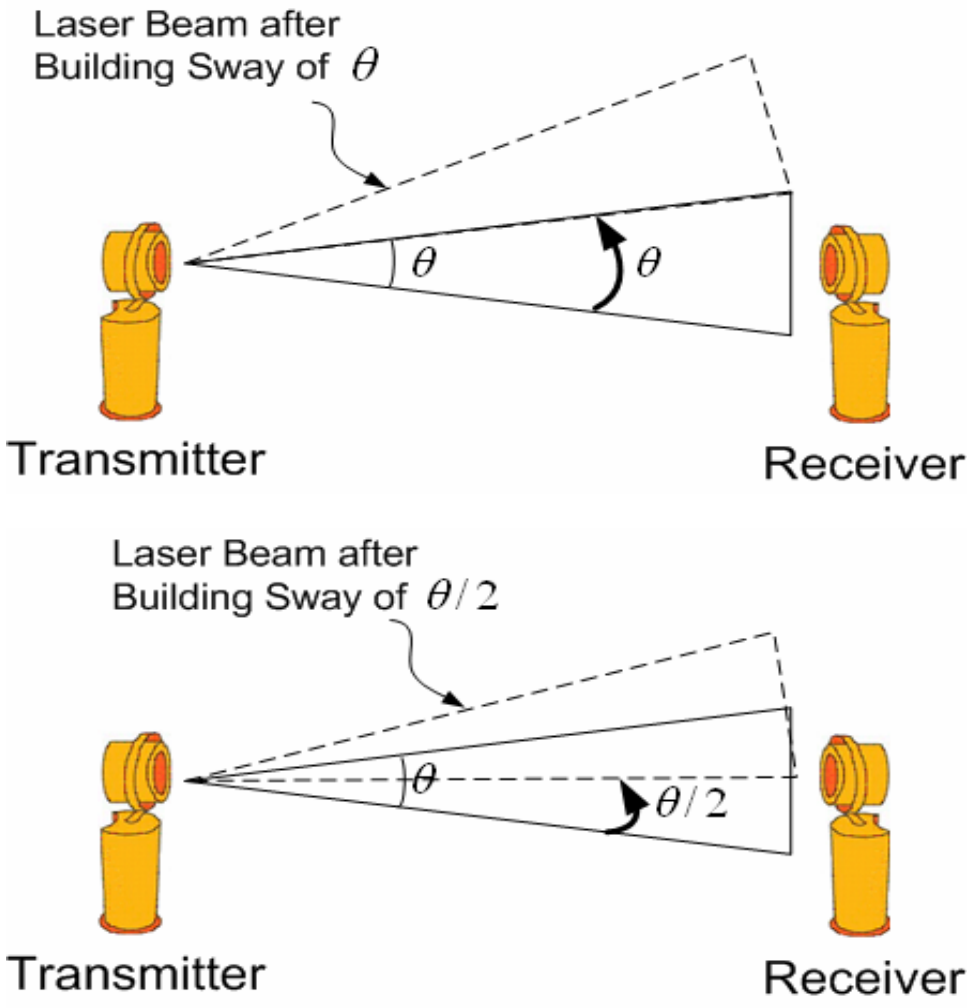

Figure 19. Laser Beam Mispointing Due to Transmitter's Building Sway [From Ref. 18.]

The divergence of the beams helps to address the beam alignment problem. Given that the beam points at the center of the receiver, and assuming usual link lengths, common beam diameters on the order of tens of centimeters passively address most of a building's movement. If the beam divergence is not expected to accommodate the movement, an active alignment system is required for avoiding an interruption of the communication link [20]. In accordance with the above, two techniques can be used as solutions to the beam misaiming problem: *beam divergence* and *active tracking*.

Following the *beam divergence* technique, systems are designed to allow the divergence of the beam on purpose, such that it forms a quite large optical cone having its

edge at the light source and its base at the receiver. Using this technique, the beam divergence alone can accommodate a significant amount of building sway, under the assumption that the receiver was initially accurately aligned to the center of the laser beam when the system was deployed [5]. However, causing a larger beam divergence is at the expense of the system's security, because a larger divergence means that the transmitted signal occupies a wider area. Thus, it can be intercepted from more locations [18].

An example of beam divergence is presented in Figure 20, where the beam diameter D_L is a function of the range r:

$$D_L = \sqrt{a^2 - r^2\phi^2} \tag{3.1}$$

where α is the beam diameter at the source and φ is the beam divergence. The use of a typical beam divergence of 3 to 6 mrad yields a beam diameter of 3 to 6 meters per kilometer of distance [16].

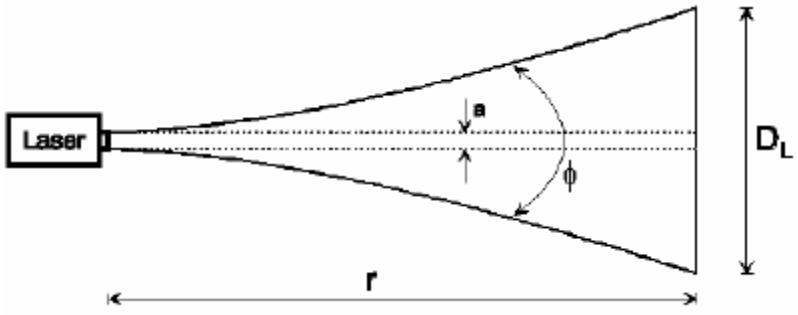

Figure 20. Beam Divergence [From Ref. 7.]

The above described wide beam transmission system, which does not include a tracking mechanism, is a cost–effective solution that is reliable for operation at moderate speeds and distances. A wider beam results in more losses in transmission power. For example, if the diameter of the projected beam is reduced by half by reducing the divergence angle in half, the total amount of power received by a receiver at a given distance increases by 6 dB. Typically, FSO systems using a wide–angle transmission without a tracking mechanism allow divergence angles ranging from 2 to 10 mrad, corresponding to beam diameters between 2 and 10 meters at a distance of one kilometer. These divergence angles are considered to provide enough misaiming angle margin, in order to main-

tain the beam on the receiving surface. It is also very important to install systems on stable locations and platforms initially. Usually, equipment mount rigidity specifications allow angles lower than the allowable misaiming angles by 1 to 3 mrad [6].

When systems are installed on very tall buildings, which move much more than the lower ones, the beam divergence technique is not sufficient to address the problem. In this case, an *active tracking* technique is required to accommodate the excessive mispointing of the laser beams. The technique has the task to automatically realign the beam to the receiver when required. This is done by auto-trackers that detect the position of the beams at the receiver and maintain them within the receiving surface [6]. Movable mirrors provide control of the direction towards which the beams are launched, while a feedback mechanism continuously adjusts the mirrors. In this manner, the beams continuously point at the receiver, whereas the transceiver is being continuously aligned. The mirrors are allowed to move up to four degrees that corresponds to 70 meters of both horizontal and vertical shifts at a distance of one kilometer. Although most of the commercial FSO systems employ the beam divergence technique, due to its lower cost, when dealing with tall buildings and long distances, this may prove inefficient. In such cases, systems using active tracking mechanisms are required [16].

4. Line–of–Site - Physical Obstructions

A solution to the link breakdown problem that FSO manufacturers have figured out is the power reduction of lasers when a link is blocked, and the retransmission in full power for a short time when the path is clear again. Although this will momentarily slow down the data rate, it will not normally cause the connection to drop out. Thus, the result will be a slower transmission rate, instead of a communication loss [16]. One of the most effective methods for recovering from temporal obstructions is error correction, whereas the deployment of physically separated redundant links is more effective against longer interruptions, for example, construction cranes [18].

G. FSO SECURITY

Since FSO systems send and receive data through the air, network operators and administrators are concerned about the security aspect of this technology. One of the main reasons is because FSO is considered to be a "wireless networking technology," a category in which security and/or interference problems are very common in radio frequency, or microwave-based communication systems, due to the wide spread of the beams. On the other hand, the direct interception of an FSO beam between the remote networking locations is difficult by default, since the beam usually passes through the air at an elevation well above ground level. Moreover, FSO systems use very narrow beams in the infrared spectral wavelength range that are typically much less than 8.727 mrad (0.5 degrees). For example, a beam divergence of 174.533 mrad (10 degrees) roughly corresponds to a beam diameter of 175 meters at a distance of one kilometer from the originating source, whereas a beam of 5.236 mrad (0.3 degrees) divergence angle, typically used in FSO systems, corresponds to a beam diameter of 5 meters at the same distance. The small diameter of the beam at the target location is one of the reasons why it is extremely difficult to intercept the communication path of an FSO system. The intruder must know the exact origination or target location of the (invisible) light beam and can only intercept the beam within the very narrow angle of beam propagation. Due to this very narrow beam diameter, capture devices must be located between the transceivers, properly aligned near the core of the laser beam and on a solid mounting structure. Therefore, interception of the beam can virtually be accomplished only at the customer location where the system is installed. Thus, a presumptive eavesdropper must have free and undisturbed access to the installation site of the FSO transceiver and be able to install electronic equipment without being observed. At that point, it would be certainly easier for them to plug directly into the network by using the existing copper-based infrastructure. In the majority of cases, the installation location does not allow free access to a potential intruder, because it is part of the customer property, such as their building's roof or an office when FSO equipment is installed behind windows. Figure 21 shows an example of a 4 mrad beam projected onto the target location where the opposite terminal is located. At a distance of 300 meters, the beam diameter is about 1.3 meters, while at a distance of

one kilometer, the beam expands to 4 meters. The photo clearly shows how extremely difficult it is for an intruder to intercept the beam. Moreover, in addition to the fact that the transmission beam is invisible and that any attempts to block the beam would occur near the FSO equipment end points, the transmission process imposes another obstacle. Picking up the signal from a location not directly located within the light path, by using light photons scattered from aerosol, fog, or rain particles that might be present in the atmosphere, is very difficult, given the extremely low infrared power levels used during the FSO transmission process. The main reason for excluding this possibility of intrusion is the fact that light is scattered isotropically and statistically in different directions from the original propagation path. This specific scattering mechanism keeps the total number of photons, or the amount of radiation that can potentially be collected onto a detector not directly placed into the beam path, well below the detector noise level [21].

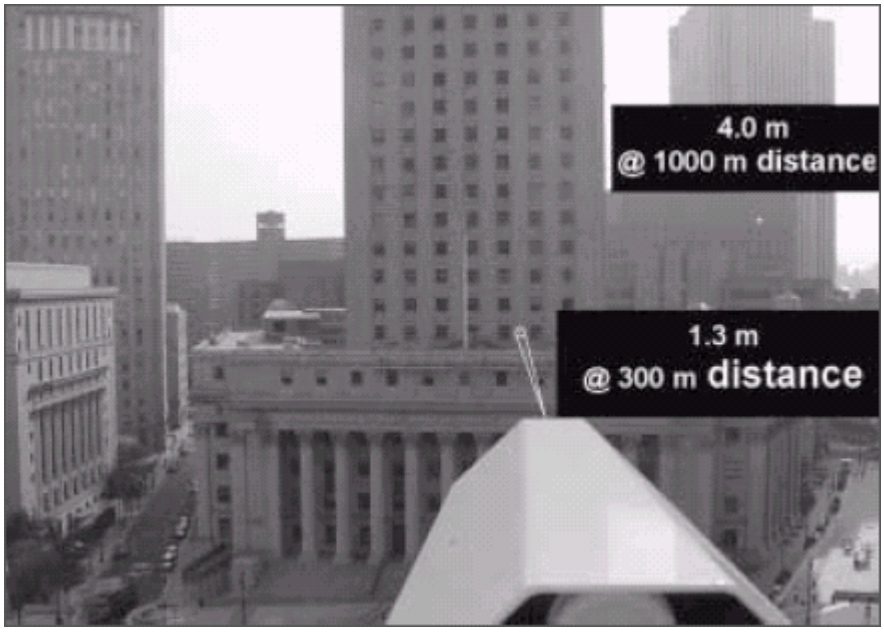

Figure 21. Example of Beam Spot Diameters at Various Distances for a Beam Divergence Angle of 4 mrad [From Ref. 9.]

In accordance with the above, FSO communication systems are among the most secure networking transmission technologies. It is extremely difficult to intercept the FSO light beam carrying networking data, because the information is not spread out in

space, but rather kept in a very narrow cone of light. Scattered light cannot be used as a method of interception. Furthermore, higher protocol layers can be used in conjunction with layer one FSO physical transport technology to encrypt sensitive network information and provide additional network security [21].

H. SUMMARY

This chapter provided an analysis of FSO networking, including its history, the technology upon which it is based, and its architecture. Additionally, factors affecting its performance and security issues were discussed.

The next chapter will present a discussion of the *IEEE 802.11 Wireless Local Area Networking* (WLAN) standard by analyzing the technology involved in wireless radio communications, and the particular specifications incorporated in the standard.

IV. THE IEEE 802.11 WIRELESS LOCAL AREA NETWORKING (WLAN) STANDARD

A. INTRODUCTION

This chapter will present a detailed discussion of the *IEEE 802.11 Wireless Local Area Networking* (WLAN) standard by providing a review of its birth, development, and dominance in the wireless market, as well as an analysis of the wireless radio technology, in general, and of the IEEE 802.11 family of specifications, in particular.

B. WHAT IS THE IEEE 802.11 STANDARD?

The *Institute of Electrical and Electronics Engineering* (IEEE) decided, in 1980, to design standards for *Local Area Networks* (LANs) and *Metropolitan Area Networks* (MANs), a project assigned the number 802. The result of the project was the standard *IEEE 802*, which was officially approved by the IEEE in 1990. Its purpose was to establish a basis for further organizing IEEE standards concerning LANs and MANs. The *Open Systems Interconnection* (OSI) model of the *International Standards Organization* (ISO) provided a framework for IEEE 802. According to the OSI model, any communication protocol is divided into seven different layers: *physical*, *data link*, *network*, *transport*, *session*, *presentation*, and *application* layers. The IEEE 802 standard defines two corresponding layers, the *physical* (PHY) and the *data link*. The *physical* layer is the equivalent of the OSI physical layer, defining what should be the physical characteristics of the medium used for transmitting data, as well as the physical signaling protocol needed for sending data through this medium. On the other hand, the OSI *data link* layer was further divided into two other layers, the *Medium Access Control* (MAC) layer and the *Logical Link Control* (LLC) layer. The MAC layer determines the protocol required to access the physical layer, while the LLC layer regulates the access to the MAC layer by multiple users. One MAC layer and multiple physical layers can form a specific access method to a network. This is the case in *Ethernet* (*IEEE 802.3*), which is a wired

LAN access method that uses *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD). The IEEE 802 family of specifications includes two more wired network access protocols, *IEEE 802.4* (*Token Bus*) and *IEEE 802.5* (*Token Ring*) [24].

On the other hand, *Wireless Local Area Networks* (WLANs) have their own physical and MAC layers, defined by the IEEE 802.11, the standard that the IEEE established for wireless networks. In other words, the IEEE 802.11 includes specifications concerning WLANs. The standard was developed by revising the IEEE 802.3 CSMA/CD protocol (Ethernet) for the purpose of allowing different devices to intercommunicate wirelessly. The specifications it includes are *IEEE 802.11*, *IEEE 802.11a*, *IEEE 802.11b,* and *IEEE 802.11g*, which all use the Ethernet protocol, but with *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) as the medium sharing mechanism. The IEEE 802.11 is similar to the Ethernet, with the exception that it provides additional physical and data link layers to the ISO's OSI model to provide Ethernet over a radio frequency (RF) [5].

The absence of a widely established standard providing common technical specifications and requirements to equipment made by different manufacturers is the main reason for the low use of wireless networks before the approval of the IEEE 802.11, although the wireless technology had long been available. Some years after the standard was approved in 1997, further ratified in 1999, devices supporting it were introduced. WLAN technology started enjoying remarkable growth in all aspects of life in the United States, Japan, Europe, and other parts of the world. Wireless networks are being deployed everywhere, offering users the ease to access computer networks services from anywhere within their WLAN coverage area, without depending on restraining wires [25]. Moreover, wireless networks find a wide range of applications in the military sector, where the virtues of quick and easy deployment, scalability, and mobility are greatly demanded.

C. THE IEEE 802.11 STANDARD HISTORY AND EVOLUTION

Before 1990, wireless products were not standardized and manufacturers made up their own standards concerning only the devices they were producing. Of course, devices

made by different companies were incompatible and could not communicate between each other. Given this situation in the wireless market, the need to add WLAN standards to the IEEE 802 family was imperative. Therefore, a working group was formed in 1990 by the *IEEE 802 LAN/MAN Standards Committee*, for the purpose of standardizing WLAN protocols and signaling. Since the working group was assigned the number 11, the name of the new protocol would be "IEEE 802.11." Using the IEEE 802 framework as a point of reference, which was used to produce LAN standards, the *IEEE 802.11 Task Group* defined the wireless physical and MAC layers, proportionally to the corresponding wired ones of IEEE 802.3. The goal of the working group was to establish a standard supporting portability and mobility, in addition to the support of devices operating in a fixed location. Although wired devices offer portability up to a point, the required physical connection and the need for a power supply constitute restrictive factors. Furthermore, the mobility of a device, implying it may be in use with full functionality while moving, creates the need of maintaining a network connection during constant motion, in addition to being self-powered. To achieve the goal of supporting fixed, portable, and mobile applications at the same time, radio waves and infrared light were chosen as the suitable transmission media for signals. However, infrared has never been largely used, because of higher cost. The fact that it requires a line–of–sight causes the necessity for more equipment, in comparison to a radio operating system, for the coverage of the same area. Consequently, the use of radio prevailed in IEEE 802.11 and its descendents, IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g [26].

The next step in the design of the IEEE 802.11 physical layer was the choice of the most adequate frequency, in order to achieve optimal use of the radio spectrum and to obtain the desired data rates. Moreover, because of the radio spectrum's regulation on a global basis, it should be an available and low–cost frequency, given that some frequencies are already allocated, while others require expensive licenses. In North America, the unlicensed 2.4-GHz radio spectrum, known as the *Industrial, Scientific and Medical* (ISM) band, is available for general use with the approval of the *Federal Communications Commission* (FCC). The 2.4-GHz frequency band, a globally regulated and widely used band, was chosen as the most suitable for low–cost and largely accepted wireless devices. More precisely, FCC specifies this band from 2.4 to 2.4835 GHz. Furthermore,

FCC ISM devices are required to operate at a maximum of 1,000 mW, and 2.4-GHz devices must use *Spread Spectrum* transmission and modulation techniques [26]. Later on, the FCC's *Unlicensed National Information Infrastructure* (UNII) frequency band (5.15–5.35 GHz and 5.725–5.825 GHz) was chosen for the operation of IEEE 802.11a. The radio frequency spectrum is shown in Figure 22.

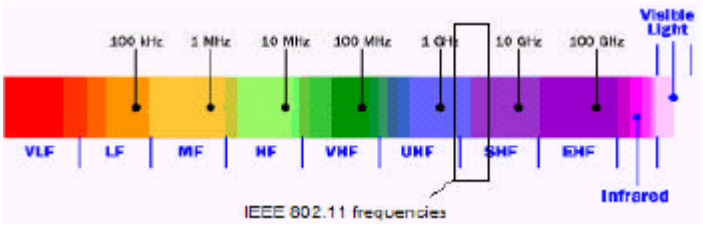

Figure 22. The Radio Frequency Spectrum [From Ref. 5.]

After several years of development, the IEEE 802.11 was finally approved and published in 1997, becoming the first globally accepted standard for WLANs, and aiming to provide a quickly deployed wireless communication solution for devices on the move [25]. The standard in its final form defines the MAC layer and three physical interfaces, supporting data rates of 1 and 2 Mbps. Infrared light was chosen as the transmission medium of the first physical layer, but was never extensively used, as explained above. Radio waves in the 2.4-GHz ISM band are used by the other two layers, with the difference that they utilize different spread spectrum transmission methods. One of them uses the *Frequency-Hopping Spread Spectrum* (FHSS), while the *Direct-Sequence Spread Spectrum* (DSSS) was the choice for the other [24].

However, the adoption of the IEEE 802.11 standard in 1997 was not enough to boost the wireless market. Data rates up to 2 Mbps were lower than those of IEEE 802.3 devices. Furthermore, the production of 2.4-GHz radio equipment was still expensive, due to the high cost of the required materials, since semiconductor technology was still under development. Due to progresses in the technology, the costs started to drop a couple of years later, together with the realization of the WLANs commercial opportunities [24]. Additionally, a revision of the standard in 1999 resolved the low data rates problem. Although the MAC layer of the original IEEE 802.11 remained practically the same, two

amendments in the physical layer resulted in new specifications: the *IEEE 802.11b*, supporting data rates of 5.5 and 11 Mbps and operating in the 2.4-GHz band, and the *IEEE 802.11a*, fundamentally different from the IEEE 802.11b, which supports data rates up to 54 Mbps operating in the 5-GHz band [25]. Generally, the IEEE 802.11b is more suitable for transaction–intensive applications, while the higher bandwidth of the IEEE 802.11a makes it more appropriate for data–intensive applications. In 2000, one more task group, the *IEEE 802.11g*, was created by the IEEE and assigned to define a standard for a data rate of 22 Mbps, which was finally extended to 54 Mbps in the 2.4-GHz band. The final version of the 802.11 family's new member was adopted in 2003.

IEEE 802.11, IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g differ in the modulation techniques they employ. The original IEEE 802.11 was limited to a speed of 2 Mbps by the chosen combination of frequency, bandwidth, and modulation. When these factors were appropriately modified, speeds up to 54 Mbps became feasible. Sophisticated spread spectrum modulation techniques, for both FHSS and DSSS, were used in an effort to optimize the use of the allocated bandwidth, resulting in an increase in data rates and range and a reduction of interference. Initially, the IEEE 802.11 supported two modulation schemes for FHSS, based on the *Gaussian Frequency-Shift Keying* (GFSK), and two for DSSS, based on the *Differential Phase-Shift Keying* (DPSK). Nevertheless, since they were insufficient for the speeds supported by the IEEE 802.11b, two new modulation techniques, the *Complementary Code Keying* (CCK) and the *Packet Binary Convolutional Coding* (PBCC), were adopted. On the other hand, the *Orthogonal Frequency Division Multiplexing* (OFDM) is the radio transmission technique chosen for the IEEE 802.11a, while the OFDM, the CCK, and the PBCC are all used in the IEEE 802.11g [24].

Advancements in radio technology and the higher data rates of the new amendments to the IEEE 802.11 standard led to the wide spread of WLANs in the late 1990's. Additionally, another factor contributing to it was the fact that, since the physical and MAC layers of the IEEE 802.11 were based on the corresponding ones of the IEEE 802.3, applications and services designed for it could be used by the IEEE 802.11 as well, so an already established market offered a base for the commercial penetration of a new standard. The realization of the 802.11 standard market potential by the manufacturers of

telecommunication equipment, computers, and semiconductors are driving large investments in the field. Commonly used *Internet Protocol* (IP) applications, like the *Hypertext Transfer Protocol* (HTTP) and the *File Transfer Protocol* (FTP), were immediately given the option of wireless connectivity. Moreover, specific services and applications for WLANs are continuously employed, and public WLANs are established in every possible location in order to satisfy the increasingly augmenting demand for Internet access. The advantages of the wireless connectivity, together with the availability in the market of low-cost devices capable of taking advantage of them, resulted in the development of applications and services in many different fields, such as education, retail, manufacturing, medicine, and the military [24].

The result of all these is that the WLAN market is currently one of the fastest growing globally, as can be seen in Figure 23.

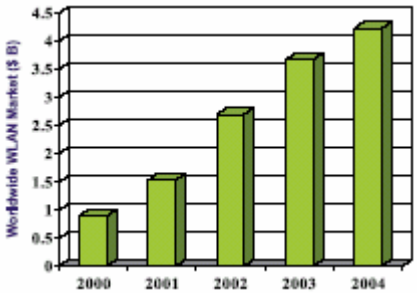

Figure 23. WLAN Equipment Market Opportunity [From Ref. 35.]

D. WIRELESS TECHNOLOGY FUNDAMENTALS

1. General Background

WLANs use electromagnetic waves (radio or infrared) to transfer data between two different locations not connected physically. The transmitted information is overlaid on a base signal, or "carrier," assigned the task to deliver energy to the other end, and is extracted at the receiver, which is tuned to the appropriate radio frequency. Signals on

different frequencies are rejected. The variation of the base signal to transfer data is referred to as “modulation” of the carrier by the transmitted information, and it may be a variation of its *amplitude* (“amplitude modulation”), *frequency* (“frequency modulation”), or *phase* (“phase modulation”) [5].

Due to physical obstacles encountered en route, a radio signal usually travels to its destination through different paths. Therefore, duplicates of the transmitted signal arrive from different directions with different propagation delays, thus reaching the intended receiver at different times, depending on the followed path. In this manner, multiple versions of the original signal, displaced in time, combine at the receiver antenna to give a resultant signal varying largely in amplitude and phase. The different phase and amplitudes of the various multipath components result in fluctuations in signal strength. This phenomenon, known as “multipath effect,” can cause the attenuation, or distortion of the original signal, since two or more versions of it may interfere between each other at the receiver. Depending on the specific amplitudes and phases, the result may be a weaker signal, or even a total cancellation of it, in case both signals have the same amplitude and completely opposite phases. Figure 24 demonstrates the different paths that versions of a radio signal can take. It should be noted that even if there is a line–of–sight between the transmitter and the receiver, multipath still takes place, because of reflections from the ground and surrounding structures [27].

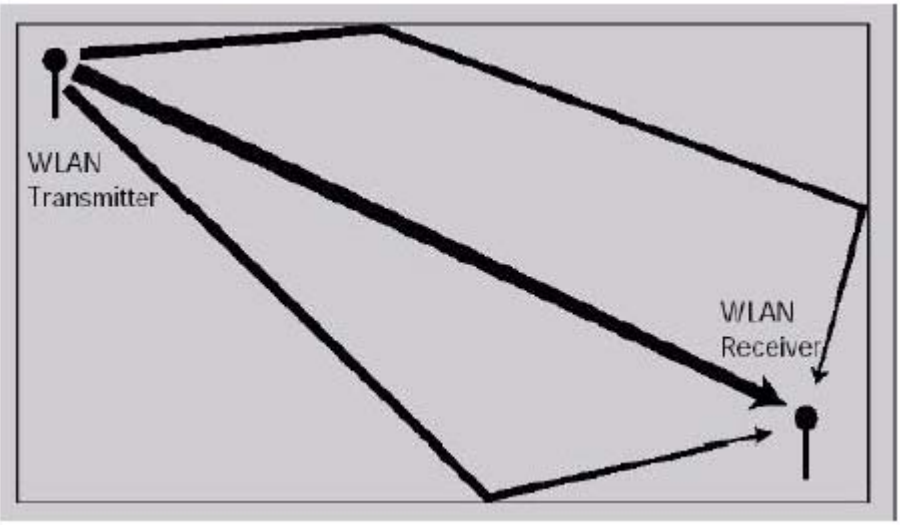

Figure 24. Radio Signals Traveling over Different Paths [From Ref. 28.]

2. Modulation and Spread Spectrum Techniques

According to the desired data rates, different modulation techniques may be chosen. In order to achieve higher data rates, more data have to be included within the same bandwidth, making these techniques more complex and costly. Furthermore, even slight alterations of the signal affect more information, creating the need for a higher *Signal–to–Noise Ratio* (SNR) at the receiver. However, since signals degrade with distance from the sender, the SNR decreases with distance as well. Therefore, the tradeoff for higher data rates is the reduction of the effective range. The modulation methods employed by the IEEE 802.11 specifications are the *Binary Phase–Shift Keying* (BPSK), the *Quadrature Phase–Shift Keying* (QPSK), the *Quadrature Amplitude Modulation* (QAM), the *Gaussian Frequency–Shift Keying* (GFSK), the *Complementary Code Keying* (CCK), and the *Packet Binary Convolutional Coding* (PBCC) [29].

The *Spread Spectrum* is a technique used to spread an information radio signal over a bandwidth wider than the one needed for transmitting a specific data at a specific rate. The reasons for doing so are to make jamming and interception more difficult, as well as to decrease sensitivity to interference. Of course, the tradeoff for obtaining these advantages is the use of additional bandwidth. The first type of spread spectrum is the *Frequency Hopping Spread Spectrum* (FHSS), while the *Direct Sequence Spread Spectrum* (DSSS) is a more recent type [30]. Both of these spread spectrum techniques are used in the IEEE 802.11 family of specifications.

a. Frequency Hopping Spread Spectrum (FHSS)

In FHSS, the additional bandwidth is used to generate a number of frequency channels, all being able to transmit the information. The information signal is superimposed on a narrowband carrier that “hops” from frequency to frequency at time intervals in the order of some hundred milliseconds in a specific pattern that only the transmitter and the receiver know. This “frequency hopping” spreads the transmitted data over the spectrum. In other words, the original information signal is broadcast over a series of

ries of frequencies, hopping from one frequency to another. The receiver hops between the same seemingly random series of frequencies in synchronization with the transmitter, and it picks the signal [31]. In the original IEEE 802.11 standard, the frequency channels are evenly spaced with 1 MHz intervals over the 2.4-GHz band, while three hopping sequence sets, from which actual hopping patterns are chosen, are assigned to each regulated area. The number of the frequency channels, the size of the 2.4-GHz spectrum, and the hopping rate are also locally regulated [29]. For example, the minimum hop rate for the United States is 2.5 hops/second, whereas the minimum hopping distance is 6 MHz in North America and Europe and 5 MHz in Japan. Moreover, each transmission must not occupy a channel for more than 400 ms. An example of an IEEE 802.11 FHSS procedure is shown in Figure 25, where a signal is split in different parts, each one of them being transmitted at a different frequency range 1 MHz wide for a time period of 400 ms. The original IEEE 802.11 standard employs two varieties of GFSK for modulation, a two–level one for transmission at 1 Mbps and a four–level one for transmission at 2 Mbps. In the first case, two different deviations from the carrier frequency are encoded with bits "0" and "1". In the four-level scheme, four different deviations from the carrier's frequency are encoded with the four 2-bit combinations [34]. A disadvantage of using GFSK for modulation is that the transmission power is used inefficiently, comparing it to the modulation techniques employed by the IEEE 802.11 specifications that use DSSS. Generally, the use of FHSS in applications requiring high data rates is limited [29].

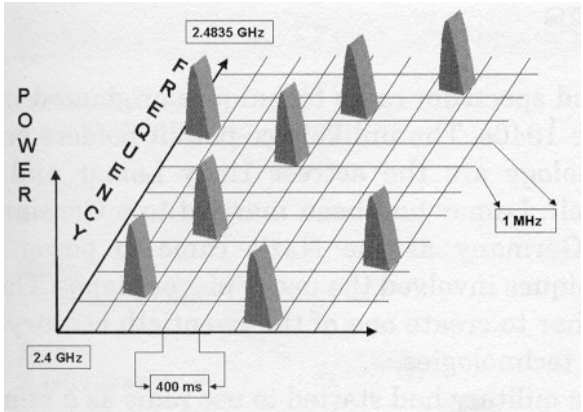

Figure 25. An IEEE 802.11 FHSS Signal [From Ref. 29.]

In order to demodulate a signal, the spreading code between the transmitter and the receiver has to be synchronized. When FHSS is used, both time and frequency have to be synchronized, which makes the process more complex.

b. Direct Sequence Spread Spectrum (DSSS)

In DSSS, the additional bandwidth is used for extra, special–purpose data, which is mixed with the transmitted information in order to distribute it over a larger frequency spectrum. Redundant bit–patterns are added to the information bit, increasing the bandwidth needed for it [29]. In other words, each information bit is represented by multiple bits in the transmitted signal. This is done through the use of a *spreading code*, which spreads the signal over a larger frequency spectrum. The bit patterns, or spreading codes, are called “chipping codes” and they differ in the rate at which they are mixed with the radio carrier, called “chipping rate.” Their length is not fixed either, as it may be up to a very long sequence. The achieved spreading of the original signal depends directly on the number of additional bits used. For example, a 10-bit code spreads the signal over a frequency band ten times wider than that of a 1-bit code [30]. An example of a 10-chip code is displayed in Figure 26, where a specific pattern of 10 bits is used to represent the original “one,” and the same, but inverted, pattern represents the “zero.” Of course, since 9 redundant bits are added to each information bit, the bandwidth required for one “new” bit is now 10 times larger than the bandwidth needed for each original bit.

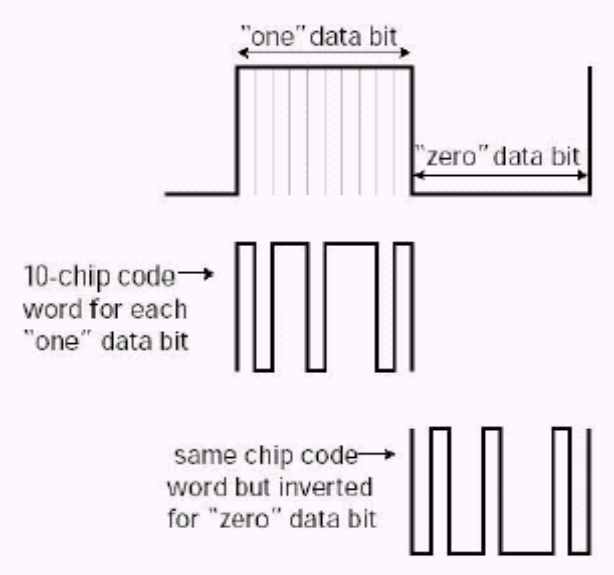

Figure 26. A 10-Chip Code of a DSSS System [From Ref. 5.]

The redundant bit patterns utilized by the DSSS systems are also called "Pseudorandom Noise codes" (PN codes), since they resemble noise to those who do not know the specific pattern used. Chipping codes permit the use of statistical methods to recover disrupted data, and result in less spectrally dense signals, since the same power is spread across a wider spectrum. Practically, this means that a spectrally sparse signal, like a DSSS one, is less probable to interfere with a narrowband signal that has higher spectral density [29]. Figure 27 displays the frequency spectrum of an IEEE 802.11 DSSS signal.

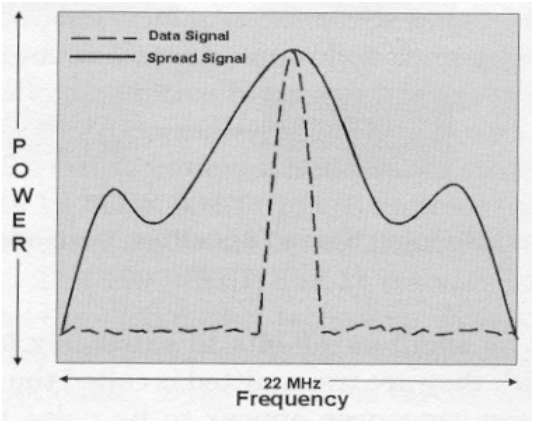

Figure 27. An IEEE 802.11 DSSS Signal [From Ref. 29.]

In DSSS systems, channels use 1-MHz carrier frequencies, like in FHSS. However, the DSSS channels are more “conventional” than the FHSS ones, since each channel is a band of frequencies occupying a range of 22 MHz. The number of 1 Mbps or 2 Mbps channels that can be used in a DSSS system depends on the available bandwidth accorded by the local responsible agency. The FCC allows 11 overlapping channels, as seen in Figure 28, whose center frequencies are 5 MHz apart. Taking into account that each channel is 22 MHz wide, only channels 1, 6, and 11 are non–overlapping, and, thus, can co-exist in the same location. Consequently, in the IEEE 802.11 specifications that use DSSS, only three non–overlapping channels of a 22 MHz bandwidth each are supported [5].

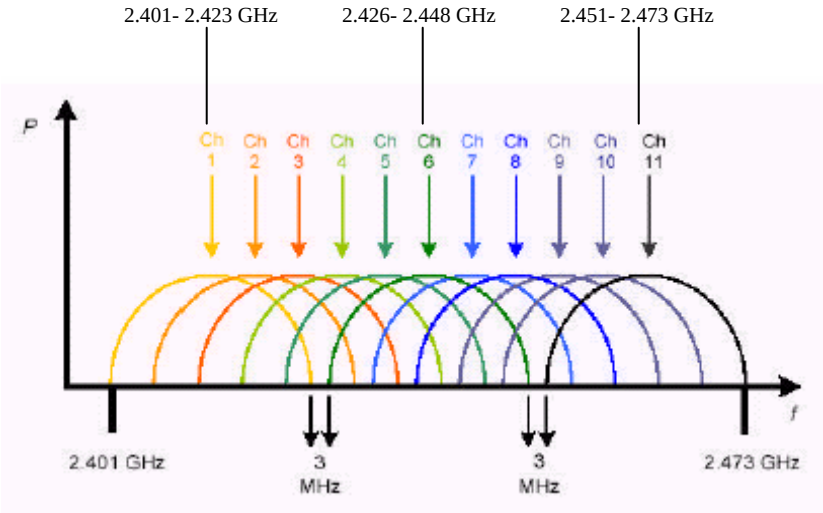

Figure 28. Channel Allocation in DSSS Systems [After Ref. 5.]

Two modulation techniques, contributing both in spreading the signal and encoding the transmitted information, are used by the IEEE 802.11 systems that implement DSSS. Both are versions of the *Differential Phase-Shift Keying* (DPSK): *Binary Phase-Shift Keying* (BPSK) and *Quadrature Phase-Shift Keying* (QPSK). The BPSK detects phase shifts of 180 degrees in the signal, representing them with “0” and “1”, and its effective data rate is 1 Mbps. On the other hand, QPSK detects phase shifts of 90 degrees, increasing the effective data rate to 2 Mbps. For supporting data rates of 11 Mbps, the IEEE 802.11b uses another modulation method, the *Complementary Code Keying* (CCK),

which has the advantage of increased resistance to the *multipath effect*. Finally, one more modulation method, the *Packet Binary Convolutional Coding* (PBCC) was added as an option to the specification, supporting data rates of 11 Mbps also [29].

The demodulation process is simpler when DSSS is employed, because, in contrast to FHSS, only time has to be synchronized, since only one frequency is used during the data transmission.

3. Orthogonal Frequency Division Multiplexing (OFDM)

OFDM uses multiple carriers for parallel transmission at different frequencies, dividing the information bits between the different subchannels corresponding to these frequencies. OFDM is based on the *Fast Fourier Transform* (FFT), a mathematical process allowing 52 *orthogonal* channels to overlap, as can be seen in Figure 29, where the peak value of each tone coincides with a zero value of the others. Thanks to this characteristic of orthogonality, these channels do not interfere with each other, despite their spatial overlapping. The use of the FFT algorithm on both the transmitter and the receiver spaces the channels as close as possible between each other, while still being orthogonal. This scheme offers a more efficient use of the bandwidth, since the overlapping of channels reduces the required spectrum [5].

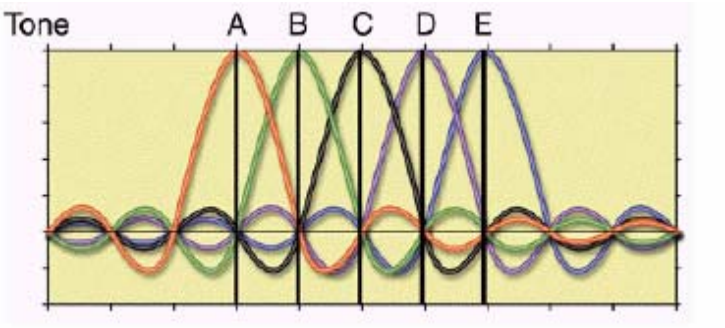

Figure 29. Overlapping OFDM Channels [From Ref. 5.]

Using OFDM in the IEEE 802.11a, the carrier frequency is divided into 52 low-speed subchannels, as seen in Figure 30. Forty-eight subchannels are used for the transmission of the information, while the remaining four are used as pilot subchannels for frequency alignment at the receiver. OFDM offers important resistance to *InterSymbol Interference* (ISI) in a multipath environment, as well as to *multipath loss* and *delay spread* [29].

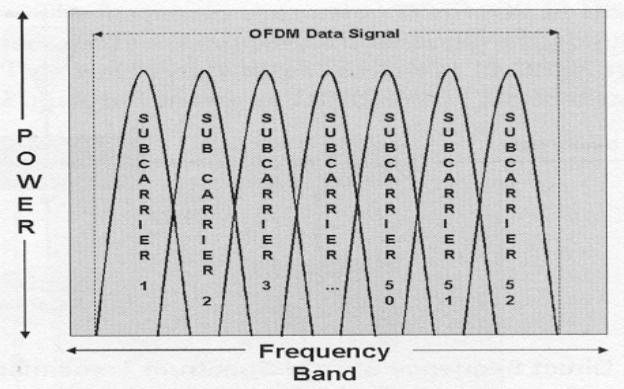

Figure 30. An IEEE 802.11a OFDM Signal [From Ref. 29.]

4. Channel Access Mechanisms

As already discussed, the mechanism allowing the sharing of a common medium used by the IEEE 802.11 specifications is the CSMA/CA, in contrast to the CSMA/CD used in wired networks.

In CSMA/CD, when a station wants to transmit, it listens to the channel to see if it is idle ("carrier sense"). If it is, the station transmits. If the channel is busy, the station continues to listen until the channel becomes idle, when it transmits immediately. If a collision is detected during the transmission, the station immediately stops transmitting, and then it waits a random period of time before attempting to transmit again [32].

On the contrary, in a wireless network, collisions cannot be detected, because a transmitting station does not have the possibility to listen to the network, since the same channel cannot be used for both transmitting and receiving. The reason for this is that

when a station is sending data, the signals it transmits prevent other signals from being received. In view of the fact that collisions cannot be detected, they must be avoided. CSMA/CA implements a method for preventing collisions, called “Distributed Coordination Function” (DCF). According to this method, when a station wishes to transmit, its *Network Interface Card* (NIC) senses the channel and only if it does not detect other radio waves above a specified threshold will the transmission take place. If it determines that the network is busy, the station “backs off” for a random time, before attempting to transmit again. The back–off time decreases at each attempt when the channel is found busy. When the back–off time approaches zero, the station gets permission to transmit. Since there is a very low probability that two stations will choose the same random back–off time, collisions can be avoided. When a station has obtained permission, it must announce its intention to transmit. Before starting to transmit, the station sends a packet called “Ready To Send” (RTS) to the receiver. Once the RTS packet arrives at the other end, and the receiver is ready to receive, it replies with a “Clear To Send” (CTS) packet that is heard by all stations within the receiver’s range, even if the RTS packet had not been heard by everyone. In that way, collisions that would have occurred in the case of a hidden sending station are now avoided. In addition to reducing the number of collisions, RTS and CTS packets help to decrease the resulting overhead in case a collision occurs. If two stations take a chance on transmitting at the same time, their RTS packets will collide and the CTS packet will not be received. Therefore, only the RTS packets will be lost, instead of the entire message [33].

E. ANALYSIS OF THE IEEE 802.11 SPECIFICATIONS

In view of the fact that the IEEE 802.11 standard works with different transmission technologies and schemes, together with the demand for higher speeds, a need for more precise specifications was created. This resulted in the introduction of the IEEE 802.11b, operating only in DSSS schemes, and supporting data rates up to 11 Mbps. It soon became the predominant specification, supported by vendors such as *Cisco*, *Lucent*, *Apple*, etc. Not very long after the publication of the IEEE 802.11b, and thanks to the

maturation of the technology, additional specifications were developed, particularly the IEEE 802.11a and the IEEE 802.11g, both supporting data rates up to 54 Mbps. Both specifications utilize an OFDM modulation scheme rather than a spread spectrum one.

1. The IEEE 802.11b Specification

The necessity for higher data rates than the ones provided by the original IEEE 802.11 led to the adoption of the IEEE 802.11b in 1999. Utilizing the same 2.4-GHz frequency band, it provides transmission speeds of 1, 2, 5.5, and 11 Mbps, and it is a natural extension of the original IEEE 801.11 DSSS scheme. Although the IEEE 802.11b works only in DSSS modes, it is backward compatible with both direct sequence and frequency–hopping 802.11 systems. Higher data rates are the result of spread spectrum modulation techniques. The occupied bandwidth is the same with the original DSSS scheme, since the same chipping rate of 11 MHz is used. The main DSSS modulation scheme that makes feasible higher speeds at the same chipping rate, and within the same bandwidth, is CCK [34], while PBCC was also included as an optional scheme.

The commercial success of the IEEE 802.11b can be attributed to several factors. The use of the same frequency with the original IEEE 802.11 made it possible to take advantage of previously completed work in the 2.4-GHz band. The modulation techniques used are simpler in implementation and are less power consuming. The use of a lower frequency makes the IEEE 802.11b less susceptible to signal degradation and enables it to cover larger areas. However, a significant disadvantage of the specification is the interference caused by the several devices that operate in the densely populated 2.4-GHz band. Another drawback of the specification is that the amount of data that can be transmitted with the 2.4-GHz frequency is limited physically, in comparison to the 5-GHz frequency that offers higher data rates. Moreover, the 5-GHz band is less sensitive to interference by other devices, since less equipment operates in this band [26].

The IEEE 802.11b specification can transfer data at indoor distances up to several hundred feet, and to outdoor distances up to about 8 to 10 miles, assuming line–of–sight. These distances depend on the obstacles encountered in the signal’s path, and the materi-

als with which these objects are made, in case there is not line–of–sight. There are eleven channels available for use. However, only three of them do not overlap. With this in mind, the theoretical maximum data rate that may be supported by these three non-overlapping channels within the same covered area is 33 Mbps. Although this drawback consists of a limitation for large–scale deployments, it may be overcome with appropriate channel spacing and separation [5].

2. The IEEE 802.11a Specification

The IEEE 802.11a specification comprises the same MAC layer with the IEEE 802.11b, including the use of CSMA/CA. The principal modifications are its operation at higher frequencies, and the use of a different radio transmission technique than those employed by the previous specifications. The IEEE 802.11a operates in the higher–frequency 5-GHz band (the FCC's UNII band), in order to fulfill the necessity for higher bit rates, and the total bandwidth is divided into three domains for a total of 300 MHz, as shown in Table 3 [5]. The operation in the 5-GHz band makes the IEEE 802.11a radically different from the IEEE 802.11, as well as from its 2.4-GHz descendents, the IEEE 802.11b and the IEEE 802.11g, offering data rates up to 54 Mbps. More specifically, the supported data rates are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps [34]. Another significant difference is that the IEEE 802.11a supports eight channels for operation, contrary to the IEEE 802.11b and the IEEE 802.11g, which both support only three non–overlapping channels.

Frequency	Max Power Output Allowed
5.15 MHz - 5.25 MHz	50mW
5.25 MHz - 5.35 MHz	250mW
5.725 MHz - 5.825 MHz	1W (outdoor only)

Table 3. Frequencies and Power Output in the UNII 5 GHz [From Ref. 5.]

Since the IEEE 802.11a operates with the same radiated power as the IEEE 802.11b, the transmission in higher frequencies decreases the achievable distances at about 3 to 5 miles. Additionally, due to the higher frequencies, the transmitted signals are more susceptible to multipath fading. In order to overcome this problem, the IEEE 802.11a uses OFDM, rather than spread spectrum schemes. Encoding is performed through a technique developed specifically for wireless indoor use, the *Coded OFDM* (COFDM), which splits a high-speed data carrier of 20 MHz into 52 low-speed subcarriers of about 300 kHz each. Forty-eight of the subchannels are used for data transmission, while the other four are used for error correction. The possible modulation techniques are the BPSK, the QPSK, the *16-level Quadrature Amplitude Modulation* (16-QAM), and the *64-level Quadrature Amplitude Modulation* (64-QAM), based on the desired rate. For example, the BPSK encodes 125 kbps for each one of the 48 subcarriers, giving a total speed of 6 Mbps; the QPSK increases the data rate to 12 Mbps; the 16-QAM, which encodes 4 bits per hertz, results in a rate of 24 Mbps and the 64-QAM allows 1.125 Mbps per 300 kHz subcarrier, yielding to 54-Mbps speeds for 48 channels [5].

Strong advantages of the technology are greater scalability, and lower interference issues, due to its operation in a much “cleaner” band, than that of 2.4 GHz.

3. The IEEE 802.11g Specification

The need for higher speeds in the 2.4-GHz frequency band led to the replacement of the original IEEE 802.11 by the IEEE 802.11b specification. However, the continuous demand for even higher data rates, and the domination of the 2.4-GHz devices in the market, resulted in the formation of the *IEEE 802.11g Task Group* in September 2000, assigned the commitment to produce a specification for data rates of 22 Mbps in the 2.4-GHz band, which would optionally be extended up to 54 Mbps. Since the operating frequencies and the available bandwidth are kept the same, more sophisticated techniques are needed for reaching the desired speeds [26]. For this reason, the basic radio transmission technique for high data rates is the OFDM.

The IEEE 802.11g specification was finally published in June 2003, and is actually a conjunction of the IEEE 802.11b and the IEEE 802.11a specifications. For the most part, the IEEE 802.11g is an extension of the IEEE 802.11b, the standard where most of the current WLANs are based. Therefore, apart from operating in the 2.4-GHz band, in the IEEE 802.11g the transmitted signal uses approximately 30 MHz, i.e., one third of the band. As a result, the number of non–overlapping 802.11g *Access Points* (APs) is limited to three, as is in the IEEE 802.11b specification. Moreover, the 802.11g equipment is backward compatible with the 802.11b devices [5]. In order to accomplish this compatibility, the IEEE 802.11g adopts IEEE 802.11b's CCK for achieving speeds of 5.5 and 11 Mbps. In view of this fact, an 802.11b radio card can, for example, directly interface with an 802.11g AP at 11 Mbps, or lower, depending on range, and vice versa. Additionally, the IEEE 802.11g incorporates 802.11a's OFDM for achieving data rates up to 54 Mbps in the 2.4-GHz band. The IEEE 802.11g also offers two optional incompatible modes for lower speeds: *Intersil*'s CCK-OFDM mode with a maximum data rate of 33 Mbps and *Texas Instruments*'s *Packet Binary Convolutional Coding* (PBCC-22) with speeds ranging from 6 to 54 Mbps.

The 802.11g devices, like the 802.11b ones, suffer from interference caused by the large number and variety of other devices also operating in the 2.4-GHz band.

Even though the 802.11b products are expected to keep dominating the wireless market for several years, the 802.11g equipment is increasingly seen as their long-term commercial successors, probably supporting the IEEE 802.11a specification simultaneously (dual band APs and devices). In this manner, the same device will support high speeds on both 2.4 and 5-GHz bands.

F. ARCHITECTURE AND SERVICES

1. WLAN Configurations

WLAN configurations may be as simple as *peer–to–peer* independent connections between different personal computers, or as complex as infrastructure networks

connecting whole buildings. Furthermore, there are two types of wireless solutions: *point–to–point* solutions are employed as bridges between different LANs, and as alternatives to cable solutions for connecting areas situated at a certain distance between each other. On the other hand, *point–to–multipoint* solutions are used for the purpose of connecting different locations to a single one [5].

A typical WLAN infrastructure configuration is based on two main components, *Access Points* (APs) and *Wireless Client Adapters*. APs have the duty to provide the interface with the wired network and manage the devices of end users, their task being similar to that of *Base Stations* in mobile networks. More analytically, APs are *Radio Frequency* (RF) transceivers that operate at a specific frequency and are responsible for moving data from the WLAN to the wired network, and vice versa. Their connection to the wired LAN is usually obtained through an Ethernet cable, and they may be placed practically anywhere it is feasible, as long as they provide the desired coverage. An AP is capable of serving about 20 users within an indoor coverage area ranging between 20 meters, in areas that include several obstacles, and 100 meters, in "clean" areas, using built–in antennas. The complete coverage of entire buildings may require, depending on a building's size, several APs, and the main idea is based on the mobile networks' cell concept. Achievable outdoor ranges may go up to approximately two miles, assuming clear line–of–sight, using custom antennas [5].

Wireless Client Adapters, on the other hand, are responsible for connecting the end users, or *Stations*, to the desired WLAN through the use of APs. The most common form of wireless client adapters are the *Network Interface Cards* (NICs), which are incorporated within the end–user devices, and provide a transparent connection between these devices and the APs [35].

Finally, for connecting backhaul WLAN traffic to the wired network, or WLAN "islands" between each other, another piece of equipment is needed, called a *bridge*.

A typical WLAN configuration is as shown in Figure 31.

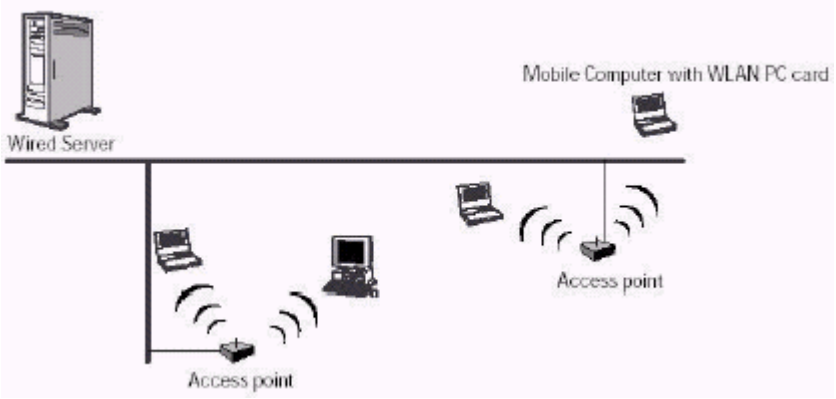

Figure 31. Typical Wireless LAN Configuration [From Ref. 5.]

As previously mentioned, the IEEE 802.11 family of specifications were established mainly for the reason of providing mobility to the users of a network, offering them the convenience to enjoy the provided services while moving anywhere within the covered area. In order to achieve mobility, flexibility in the network topology and scalability are essential. Indeed, the 802.11 specifications provide the possibility to potential wireless users to become part, for any period of time they wish, of a given network, with the only requirement to possess within their device a NIC capable of setting up a radio communication interface with the responsible in the particular area AP. As long as a device is within the AP's transmitting/receiving range, it can establish a wireless connection with the wired network to which the AP is connected [5].

2. The IEEE 802.11 Standard Architecture and Services

a. Architecture

The architecture of the IEEE 802.11 specifications is based on a number of components and mechanisms that interact between each other for the purpose of providing station mobility transparency to the higher layers of the network stack. The hierarchical network architecture supported by the IEEE 802.11 allows the configuration of WLAN equipment in many ways, thus providing the desired flexibility [26].

The *Basic Service Set* (BSS) is the fundamental type of WLAN configuration supported by the IEEE 802.11 specifications, and is similar to the cell concept in mobile networks. A BSS is the smallest building block of a WLAN, comprising stations in close proximity between each other that implement the same MAC protocol and share the same wireless medium. The relation between BSSs and stations is not permanent, but dynamic, as stations come within and out of a BSS's range [34]. Propagation and interference issues that affect a radio signal's strength dictate the maximum operating distance between stations. The most primary form of a BSS is the *Independent Basic Service Set* (IBSS), which is a simple isolated network supporting communication only between stations that are part of the network. Communications between these stations are performed directly (peer–to–peer), with the use of wireless adapters, without any kind of centralized coordination by a master station [26]. Any time different wireless adapters are the one within the range of the other, they can communicate wirelessly, in an *ad hoc* manner. A typical IBSS can be seen in Figure 32.

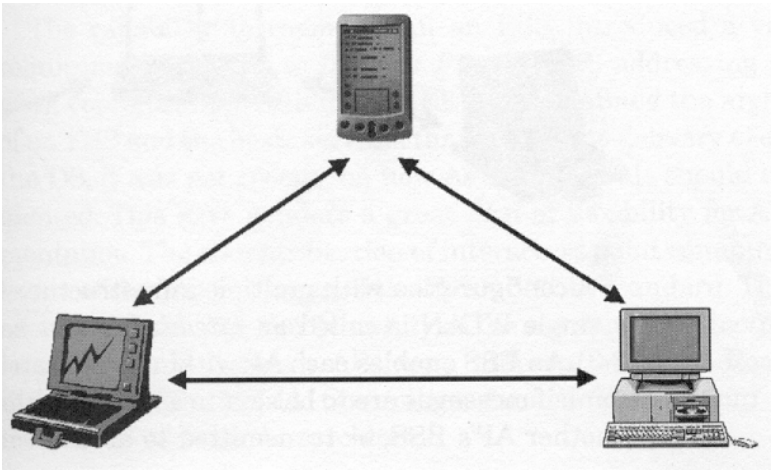

Figure 32. An Independent Basic Service Set [From Ref. 26.]

However, a BSS may use an AP, acting as a *bridge*, to connect to a *Distribution System* (DS), a medium used as mediate for connecting BSSs to each other, to wired networks, and vice versa. To accomplish this task, the DS, which may be a wired network, a wireless one, or a switch, carries out all communication between the APs, acting as a backbone for the WLAN [25]. When an AP is used, the BSS is called "infrastruc-

ture.” The MAC protocol can be either totally distributed, or managed by the AP, through a central coordination function incorporated within it [34]. In this case, the use of the AP, in addition to gateway functionality and buffering, provides centralized distribution, since all communications performed within the BSS have to go through the AP. The gateway functionality of an AP allows connections to wired LANs, or to other external networks, while its buffering functionality provides power management for self-powered devices. Moreover, the transfer of data among stations through an AP practically doubles the covered area, since the AP virtually acts as a repeater. Depending on the extent of the area to be covered, a different number of APs is required, in order to cover it efficiently. An example of an infrastructure BSS is displayed in Figure 33 [26].

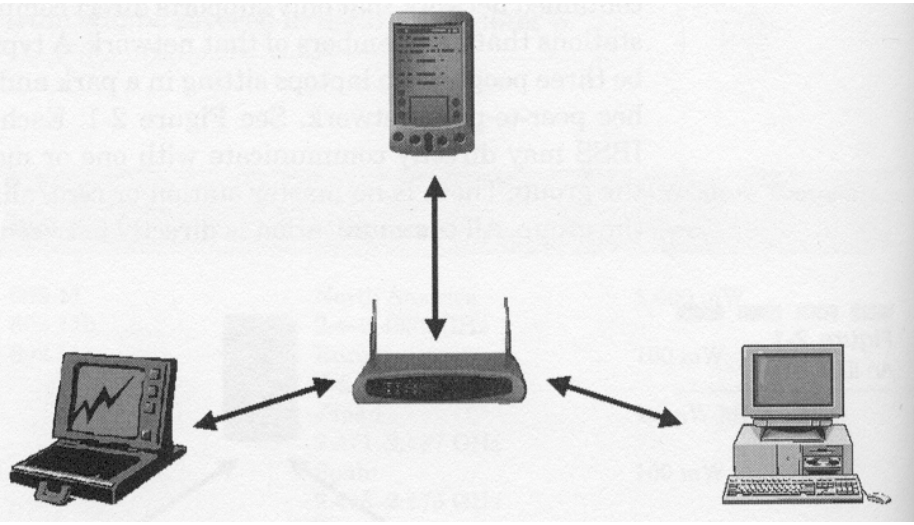

Figure 33. An Infrastructure *Basic Service Set* [From Ref. 26.]

The next level of configuration is the *Extended Service Set* (ESS). An ESS consists of two or more infrastructure BSSs, each one of them being controlled by one AP. The reason for using an ESS is to extend the covered area of a WLAN by connecting new BSSs to the ones it comprises already, through the use of APs. The existence of multiple BSSs is transparent to the users, to whom an ESS appears to function as a single WLAN. Therefore, a user, or station, may move seamlessly across areas covered by different APs, within the ESS’s range, thus the greatly desired mobility can be materialized [30]. An ESS seems to be a single MAC layer network to any wired network communi-

cating with the WLAN of which this particular ESS is part, and all its stations look like fixed ones, no matter if they are moving or not. In this manner, the wireless connectivity is hidden from the wired networks connected to this specific WLAN. APs communicate between each other, their task being to coordinate and forward the data traffic among themselves and among stations [25]. More precisely, with the use of an ESS configuration, every AP is responsible for determining if received data must be routed to stations belonging to the BSS it controls, sent to another BSS–member of the ESS, or forwarded to an external wired LAN, or other network. This mechanism is provided by the DS, which is independent of the medium connecting an AP to the other elements associated to the DS. Thus, while the AP communicates with the stations within its BSS using radio signals, it has the possibility to communicate with other APs and external networks through radio transmission, as well, wired LAN, or any other kind of available medium [26]. DSs are usually wired backbone LANs, although any communication network may serve the purpose. Two examples of primary ESS configurations are shown in Figures 34 and 35. Note in Figure 34 that APs act as stations, also, in addition to providing BSS services to their BSSs. In more complex configurations, different BSSs may overlap, meaning that stations can be part of multiple BSSs [34].

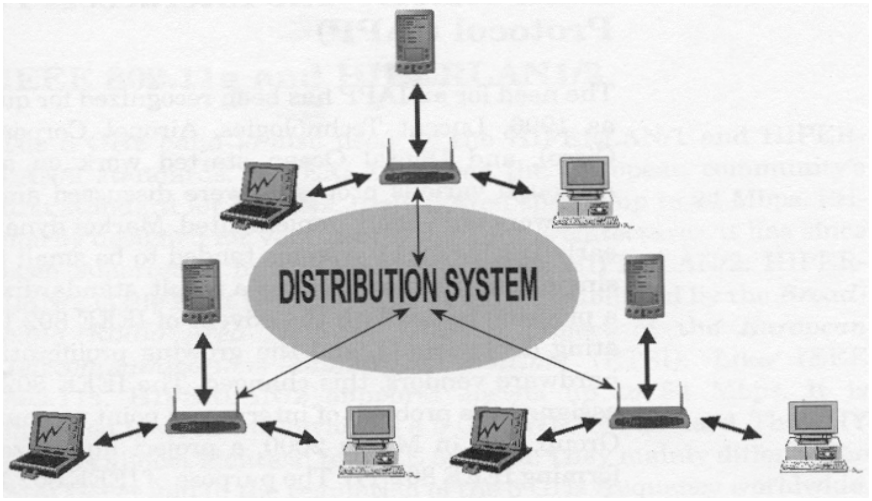

Figure 34. An Extended Service Set [From Ref. 26.]

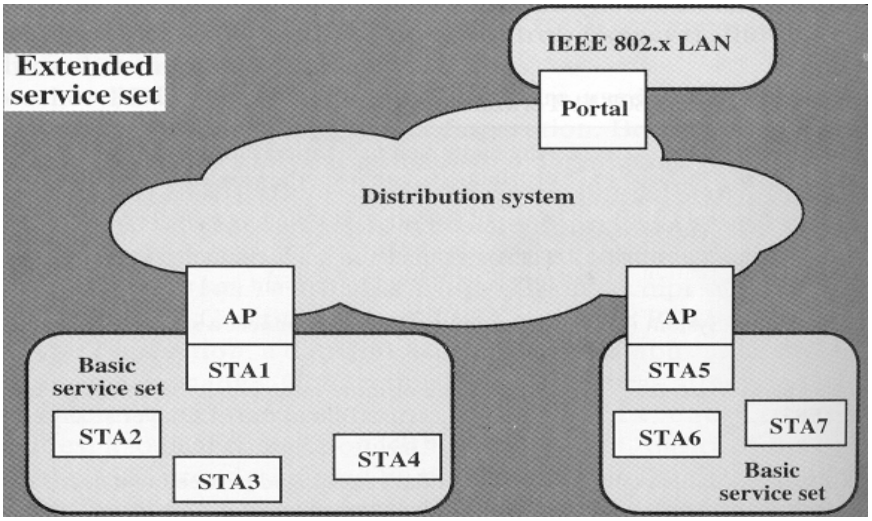

Figure 35. Basic IEEE 802.11 Architecture [From Ref. 34.]

b. Services

All the IEEE 802.11 specifications have the same MAC layer, which specifies the functions and protocols required for the control and access of the physical layer. In other words, the MAC layer manages the transfers of data from higher–level functions to the physical medium. Nine logical services, needed in WLANs for providing functionalities equivalent to those of wired LANs, are included in the MAC layer architecture: *authentication,* which establishes the identity of a station; *deauthentication,* which removes an authentication; *association,* which maps a station to a specific AP; *disassociation,* which removes an association; *reassociation,* which transfers an association between different APs; *privacy*, which prohibits unauthorized stations to access data; *distribution,* which is responsible for the transfer, through the DS, of data among stations; *data delivery,* which supports data transfer between stations, and *integration,* which supports the transfer of information between the DS of an 802.11 LAN and a LAN that does not support the IEEE 802.11 standard. This functionality is performed through a station called a “portal.” These services are all used by APs, which act as part of the DS, while

stations use four of them, *authentication*, *deauthentication*, *privacy* and *delivery* [32]. These services are called *Stations Services* (SSs), and their purpose is to provide security and data delivery services to the WLAN [25].

G. PERFORMANCE ISSUES

A relationship exists between a signal's strength, the transmission rate, and the attained distance. Theoretically, with a given signal strength, the transmission rate decreases, as the distance increases. Moreover, the propagation of a signal also depends on its frequency. Lower frequencies generally achieve longer distances without severe attenuation, but higher frequencies can carry more data [26].

1. Path Loss, Multipath Loss and Delay Spread

The transmission of a signal in a wireless environment has to face *path loss* or *multipath loss. Path loss* is the loss of the signal's power as the distance between the AP and the station (user) increases. A vast variety of physical obstacles along the signal's path contribute to path loss. The transmission frequency can also influence path loss, in view of the fact that higher frequencies cannot achieve the same ranges with lower ones [33].

The *multipath effect*, taking place when radio waves are reflected or pass through objects such as walls and furniture, cause the attenuation, or *multipath loss*, of signals at a degree that depends on the specific types of materials they encounter. Radio waves cannot penetrate some materials, whereas other materials may or may not allow radio waves to pass through them, depending on the waves' frequency. Low–frequency signals may pass through some types of walls, while higher–frequency signals may be reflected by the same wall, losing part of their energy. Due to this environmental variability, it is very difficult to estimate the maximum distance coverage and data rate of 802.11 systems [29].

The main problem caused by multipath is *delay spread*. *Delay spread* is the echo effect created when signals arrive at slightly different times at their destination, in accordance with the fact that they travel over different paths and at different speeds, since they encounter a different number of reflections. The delay–spread phenomenon can cause destructive interference between signals, since the current signal can be corrupted by the echo of a previously transmitted one. The possibility of this type of interference increases with the increase of the transmission rate. Due to the fact that a signal reaching the receiver's antenna results from different versions varying in amplitude and phase, the output of this combination may be a signal with a weakened strength, in comparison to the original one. For this reason, APs are responsible for demodulating and decoding the received signal properly, in order to recover the initial one sent. Having this in mind, there are DSSS products that attempt to solve the multipath loss problem by using various techniques such as diversity antennas, or signal–filtering and decision–making software capable of selecting the better signal [33].

2. Radio Interference

Radio interference is caused by other signals operating in the same frequencies as the ones utilized by a given system, and the result is the disruption, or even elimination, of the system's signals. With the use of the CSMA/CA mechanism in the IEEE 802.11 specifications, a station's NIC will prevent an intended transmission if the channel is found busy, i.e., in the presence of any radio signal above a certain threshold. Thus, any interfering signal above this threshold will make the NIC consider the medium as occupied. Therefore, the IEEE 802.11 MAC protocol identifies a strong interfering signal as an 802.11 transmitting station, forcing all stations in the 802.11 network to wait until the ending of the interfering transmission. On the other hand, when 802.11 stations are transmitting, an interfering source may begin sending data as well, since it is not constrained by a similar protocol. If this happens, it is probable that the intended 802.11 receivers will receive the transmitted data with errors. In this case, according to the protocol, the receiver will not sent an *acknowledgement* (ACK), so the transmitting station has to resend its data, resulting in overhead in the network that, in turn, will cause delays,

and, thus, degradation in the system's performance. When such a situation is acknowledged, there is a provision for stations to automatically switch to a lower bit rate, or cease their transmissions and wait until the unwanted source stops sending data [33].

In order to address the problem, and to decide which are the proper locations to install the APs during the settling of a new WLAN, an RF survey is required. The use of a spectrum analyzer allows the tracing of channel usage and overlap by displaying the amplitudes of existing signals in all channels. Therefore, it is possible to detect the interfering sources, so the 802.11 signals may be isolated from them, and interference can be eliminated. Taking into account the limitation that only three APs, in 802.11b and 802.11g networks, or eight APs, in 802.11a networks, can operate in different channels at the same covered area, this approach offers the possibility of proper channel planning for achieving wider coverage [33]. Furthermore, the use of devices operating in the 2.4-GHz band such as cordless phones or *Bluetooth* devices close to 802.11 stations or APs must be avoided.

H. SECURITY

Security issues in wireless networks are closely related to the nature of the medium used in wireless communications. Given that the transfer of data is performed over the airwaves, transmissions cannot be constrained within controllable physical boundaries. Furthermore, typical RF and microwave antennas used to interconnect two remote networking locations in a point–to–point architecture spread out the radiation over angles between 5 and 25 degrees. This wide spreading of the beam in microwave systems, combined with the fact that microwave antennas launch a very high power level, is the main reason for security concerns [21]. Therefore, information carried by radio waves may be passively intercepted, even though a potential eavesdropper has to be located close to the network [36].

During the first years of the wireless era, companies and organizations that installed wireless networks continued to implement the same security policies as with their already implemented wired Ethernet networks, because they had not realized the particu-

larities involved in the wireless technologies. However, the existing policies proved to be insufficient for radio transmission in the open air [25]. Consequently, many vulnerabilities and security holes have been discovered in the IEEE 802.11 security protocol over the years.

1. Wireless Security Risks

Stations and APs in WLANs exchange specific frames called “beacons” for declaring their presence on the airwaves so that authorized users may access the network. However, beacons are transmitted in the open air without any privacy functions, so they are susceptible to potential interceptions and, since they include the required information for the legitimate users to access the network, their interception may allow this access to unauthorized users [25].

The increasing acceptance of WLANs in companies and organizations, as well as the wide spread of affordable wireless devices in the market, gave birth to another problem. Employees often connect their personal devices to their company’s infrastructure network, without the administrator’s permission. Even worse, a branch of the organization may install wireless network equipment in the main network without the knowledge of the parent company [25]. For all that, the irresponsible use of wireless devices represents very serious security risks for organizations.

Given that WLANs operate at lower data rates, compared to the wired networks, and the available capacity is shared among multiple stations, a busy network is susceptible to “denial of service” attacks. Such an attack could be launched from a wired network at a much greater speed than the wireless channel can handle. This danger may be reduced if APs and stations are placed close to each other, in order to allow the use of lower signal strengths [25].

2. The IEEE 802.11 Standard Security Mechanisms

The IEEE 802.11 standard provides specifications at the physical layer and the MAC layer to implement security through the use of *authentication*, *association,* and *privacy* services. More analytically, the standard implements three basic security mechanisms.

a. Service Set Identifier (SSID)

The first mechanism is the *Service Set Identifier* (SSID), an alphanumeric code entered into all stations and APs participating in the same WLAN, which can be used as a password between a station and its corresponding AP, or as a broadcast location identifier in a public network. By default, the SSID is periodically broadcast by the network's APs. In many cases, a network's administrators have the possibility to disable the default broadcast of the SSID, forcing the users to know the network's name or, otherwise, to possess appropriate software able to capture this information. However, since the SSID is sent in cleartext as a reply to a probe from a station even if it is not broadcast, this is a quite weak security mechanism. Indeed, software tools able to detect this are already available, and, thus, inform the user for all the networks in the area [36].

b. MAC Address List

The second security mechanism is the *MAC Address List*, a list of the wireless NICs' MAC addresses, each one associated with a given AP. The list can be manually entered and managed, so that access can be limited only to the addresses included in the list. Nevertheless, this mechanism is vulnerable as well. Given that the MAC addresses are transmitted in cleartext also, an eavesdropper may capture them and, once this is done, he may obtain access to the network, since just one known valid MAC address is sufficient for configuring a wireless NIC [36].

c. Wired Equivalency Protocol (WEP)

Due to the ease with which data transferred through radio waves can be intercepted, the IEEE 802.11 Task Group specified a protocol attempting to address some of the security risks, the *Wired Equivalency Protocol* (WEP), an encryption algorithm that is the third security mechanism of the standard. The WEP is implemented at the data link and physical layers, having the task to provide some protection against data interception and alteration. When the protocol was selected, it was believed to be reasonably efficient, although it is the only available one for the standard. Furthermore, it is optional and turned off by default in most of the 802.11 devices sold on the market. Even when the service is enabled by the vendor, the device is usually configured with the "keys" the vendor uses in all the devices sold. Therefore, a user who wants to implement encryption has to activate the service, if it is not activated, and change all the default keys to the proper ones, before starting to participate in wireless data transfers [25]. The standard allows the specification of up to four keys, and provides external key management services for distributing them to the stations. A major disadvantage of the method is that the keys are controlled by the network's administrators, remaining static until manually changed by them. In case a station is accidentally lost, or stolen, the keys have to be changed for all stations, which is very hard to do in a large network [36].

I. SUMMARY

This chapter provided an analysis of the IEEE 802.11 specifications, including the reasons involved with their use, their history and evolution, the technology behind them, and their architecture and services. Additionally, performance and security issues were discussed.

The next chapter will examine and compare Free Space Optics and IEEE 802.11 technologies as potential solutions to the "last mile problem".

THIS PAGE INTENTIONALLY LEFT BLANK

V. FSO AND THE IEEE 802.11 WLAN STANDARD AS POTENTIAL SOLUTIONS TO THE "LAST MILE PROBLEM"

A. INTRODUCTION

This chapter will present an examination of *Free Space Optics* (FSO) and *IEEE 802.11 Wireless Local Area Networking* (WLAN) technologies as potential solutions to the "last mile problem," and a comparison between them.

B. FSO IN THE "LAST MILE"

Following the evolutions in optics' and lasers' technologies and the consequent lowering in cost, FSO was transformed from a short–term solution for short–haul bridges to a significant alternative able to provide the high–bandwidth expectations. The huge demand for higher speeds in the metro networks has caused a "connectivity bottleneck," forcing service providers to find a cost–effective, reliable and quickly implemented solution for connecting their end user customers, at a time when investment money is hard to find. FSO technology is a candidate to solve the problem, since, as an optical technology, FSO may be a natural extension of the metro optical backbone network, thus bringing optical capacity to the edge of it [11]. In this context, nowadays FSO technology is increasingly attracting service providers and carriers. Many of them are already using FSO not only as a broadband backup, but also as a viable "last mile" technology. Moreover, in addition to providing "last mile" connections, FSO equipment is more and more deployed for numerous other applications, such as mobile networks assist, wired networks backup, and emergency relief. According to market experts, FSO global equipment revenues are expected to reach two billion dollars in 2005, compared to one hundred million dollars in 2000 [7]. A key factor driving the market's growth is its evolution to higher speeds and carrier–class reliability. Due to its several and important advantages, FSO has a high potential to resolve the "last mile problem."

1. FSO Benefits

FSO has significant advantages compared to fiber. Unlike fiber, if customers wish to cancel the offered services, FSO equipment can be redeployed, which makes it a “zero sunk–costs” solution. It also offers carriers an important profit potential, given its low cost and installation time, whereas at the same time, they can take advantage of the high–capacity capabilities of optical transmissions. If the requirement of *line–of–sight* is met, full duplex optical transmissions over metropolitan distances from some city blocks to a few kilometers are feasible at speeds on the order of gigabits per second. Of course, these data rates are more than satisfactory for supporting voice, data, and video traffic. Using FSO technology, operators have the opportunity to accelerate their deployment of metro optical networks and extend the use of this capacity to any user desiring it [22]. Indeed, because it is not needed to open trenches for laying cables, licenses concerning digging up streets are not required and the installation for a new customer can be completed within days. Moreover, FSO systems use high frequencies that are located in the unregulated section of the spectrum. The *Federal Communications Commission* (FCC) does not regulate the use of frequencies above 300 GHz; thus, unlike in most lower–frequency microwave systems such as *Local Multipoint Distribution Services* (LMDS), no operating licenses are required for FSO communications, which is also true worldwide. In view of the fact that it is not necessary to buy an expensive spectrum, the cost and time it takes to render a system operational are substantially reduced. Thus, FSO systems are cost and time attractive, since they can be installed within one or two days, or even within hours, costing approximately $20,000 per building, compared to fiber optic systems that need months to be installed and cost $200,000 per building [13]. Therefore, more and more companies are involved in the development and supply of systems used in laser links in a growing number of applications around the world, attempting to close the current connectivity gap between the core metro optical networks and the access optical network.

The properties of the FSO technology provide for the ability to connect users to a local network, even inside buildings. There is also the option to accomplish communications between the buildings of a campus, where it is desirable to plug two sites into a lo-

cal network, rather than to connect them to the long–distance backbone. Optical wireless is characterized by simplicity: connect a laser transceiver to a network, target the transceiver located in another building, and transceivers at both ends are just plugged into the local network hardware.

2. FSO Limitations and Challenges

Unfortunately, FSO do not have only advantages. Apart from the similarities that fiber optic cable and free space optical wireless share, they differ in the way they transmit information, since fiber uses a quite predictable medium and FSO uses an open medium, subject to outside disturbances. Transmission integrity is relatively predictable when light is transmitted through fiber, but when it is transmitted through the air, which is the case in FSO systems, it must deal with the atmosphere, a complicated and not easily quantifiable factor. The result is the unpredictability of laser power attenuation in the atmosphere, one of the most important differences between free space and fiber optic transmissions. While attenuation in fiber optic cables occurs at a constant and predictable rate, atmospheric attenuation is difficult to predict, since it is variable and weather–dependent [23].

In satellite communications, laser beams must be enough narrow (a few μrad) to transport as much light power as possible to destinations at very long distances away. For this reason, the precise pointing of laser beams is crucial; even a slight misalignment of a narrow beam may cause the disruption of the communication link. Although in FSO networks the lengths of the communication links are much smaller, the exact pointing of the beam is still very important [6].

Paths in FSO communications have to be free from any physical obstructions, because light propagates in a straight line and does not have the capability to pass through solid obstacles. Thus, a line–of–sight between a transmitter and a receiver is needed, which means that they must be able to “see” each other without interference. Unobstructed line–of–sight between two communicating sites is a strict requirement for FSO systems, even stricter than in microwave systems.

3. FSO Performance in Terms of Availability and Link Range

Because of the fact that achievable link distances and link availability ("uptime") are significantly affected by the climate conditions in the area in which a system is located, maximum *link ranges* is one of the major issues concerning FSO communications. Even the use of much higher power lasers does not help to increase the attainable ranges proportionally, especially in very adverse weather conditions. The main issue here are the weather related outages that are considered acceptable. The more disconnection time can be afforded, the longer can be the link ranges of the network. For example, if communications' discontinuation, due to the weather, up to eight hours per year (i.e., 99.9% availability) can be afforded, the permissible link ranges may be much longer compared to those of another situation allowing discontinuations of only five minutes per year (i.e., 99.999% availability). In a more detailed example found in Ref. [37], a typical FSO system link margin of 40 dB requires link ranges of 200 meters for 99.999% availability in a foggy location. Most commercial FSO systems have link margins of around 35 dB to 40 dB. By contrast, if the desired probability is only 99.9%, at the same location, the link ranges are allowed to be up to one kilometer. Furthermore, a much more powerful FSO system with a link margin of 60 dB requires link ranges of 220 meters for 99.999% availability, giving a link gain of only 20 meters in comparison to the 40-dB system. However, for 99.9% availability, the length of the links may be up to 1500 meters. This disproportional difference is due to the high attenuations in the presence of fog, which can reach 100 dB/km in thick fog, and over 300 dB/km in dense fog. Under these circumstances, in a dense fog situation and given 99.999% availability, even an ultra–high performance 60-dB system can maintain a link of only a couple hundred meters. Contrary to this reality, it is often claimed by FSO manufacturers that their products may reach link ranges of three or more kilometers. In practice, most of the commercial FSO systems cannot maintain a link at such distances, or can only do it under favorable weather conditions. This is because significant link margin is lost at these ranges, so there is no available link margin to overcome fog, not even light rain in some cases. Of course, when designing a system, it is the worst situation that has to be considered and not the best one, especially when taking into account that locations with "clear air" year round is an unrealistic assumption. Start-

ing from the desired link availability for a specific FSO system, the attainable link ranges depend on the area to which the system has to be deployed. In any case, for most applications, FSO link ranges may be between 200 and 500 meters, no matter which type of laser is used, due to physics limitations. Nevertheless, in applications where FSO systems are used as a lower availability backup to other, higher availability technologies (e.g., fiber connections), link ranges of up to one or two kilometers may be allowed [37].

C. THE IEEE 802.11 STANDARD IN THE LAST MILE

Wireless networking is continuously evolving, since its beginning with a data rate of 2 Mbps (IEEE 802.11) to 54 Mbps (IEEE 802.11a and IEEE 802.11g) at present, making 802.11 technology a considerable solution for high–speed Internet, and a potential choice for the "last mile" [5]. Although the IEEE 802.11 standard was designed for indoor data transfer, by using external antennas and signal amplifiers, together with the same indoor equipment, WLANs boundaries can be extended to cover larger areas, thus allowing the technology to be used as a "last mile" solution. Thus, a continuously increasing number of large and small organizations, enterprises, and institutions worldwide are deploying WLANs for *point–to–point* and *point–to–multipoint* data communication in different environments, thanks to the flexibility and modularity of WLANs design [25].

1. The IEEE 802.11 Standard Benefits

The fact that the standard frequency ranges for WLANs (2.4-GHz and 5-GHz bands) are part of the license–free portion of the spectrum means lower costs in services and equipment, and has led to the adoption of products using the technology in an extended range of uses [5]. The technology has already demonstrated its reliability in data transfer over long distances by its broad use in widespread areas, through the use of wireless routers that bridge two or more WLANs/LANs. Moreover, *Wireless Internet Service Providers* (WISPs) use the technology to offer their customers wireless broadband Inter-

net access in areas where other broadband technologies are not feasible. Home users willing to have broadband services available everywhere in their house, and the possibility to share the use of different computer devices without the restrictions of cables, constitute an important part of WLANs clients. Furthermore, the availability of Internet and e-mail connectivity by using laptops and *Personal Digital Assistants* (PDAs) equipped with *Wireless Network Interface Cards* (WNICs), is being extended to users on the move, through the installation of wireless "hot spots" in airport terminals, train stations, university campuses, hotels, coffee shops, and other public meeting spots, where Internet users demand access [25].

Therefore, WLANs are being adopted on a large scale in the corporate, public and *Small Office Home Office* (SOHO) environments, giving users the opportunity of easy and cost–effective access to the Internet and computing resources. WLANs based on the IEEE 802.11 standard are a fast and inexpensive way to provide broadband connectivity wherever home users, employees, or travelers request it. Thus, 802.11 WLANs offer a successful solution to the broadband connectivity problem of end–users, while eliminating the need to deploy fiber cables, cable access points or Ethernet in buildings, and providing the flexibility of expansion [35]. The successive updates and revisions of the standard are the result of these virtues of the technology. At the same time, manufacturers are competing to fabricate products following the latest specifications, leading the market to lower prices, while continuously upgrading the performance of the wireless devices.

2. The IEEE 802.11 Standard Limitations and Challenges

The environment within which radio signals operate makes them susceptible to diverse conditions that influence their performance, quality, and range. Unfavorable phenomena, such as *multipath*, *fading*, and *interference*, may be caused by objects within the covered area, other physical characteristics such as building materials, environmental conditions, and the presence of other radio signals. All these factors affect the propagation of radio signals. Furthermore, since the environment is not static, the movements of objects, people, or the nodes themselves may result in variations in the signal. Due to all

these adverse conditions, the strength of a signal transmitted between two nodes may fluctuate severally, even on a per–packet basis. Since the above fading factors cause transmission errors that the system must correct, additional overhead is added to it [33].

The most important challenge in WLAN deployments is *Radio Frequency* (RF) interference, caused by unwanted radio signals that may disturb the operation of a system. As explained in the previous chapter, in an 802.11 network a station is allowed to transmit only if no other source does. When a station is transmitting, any other station desiring to send its data has to wait until the channel is free. The problem with this provision of the IEEE 802.11 MAC protocol is that a strong enough interfering radio signal may appear as a transmitting 802.11 source, which results in real 802.11 stations waiting until the interfering source stops transmitting. If an interfering source appears during an 802.11 station's transmission, in most cases the station will continue to send data, but at a lower data rate that will slow down the operation of the system. In more uncommon cases, the 802.11 station will even stop its transmission until the medium is free again, a time period that may be unpredictably long. Consequently, the existence of interference sources, particularly in enclosed areas, competes with the legal 802.11 ones, and may decrease both the throughput and the availability of a wireless network to a high degree [38]. The interference level increases conversely to the distance, so it becomes a major issue in the case of 802.11 and non–802.11 devices close to each other.

WLANs based on the IEEE 802.11b and the IEEE 802.11g specifications are more vulnerable to radio interference compared to 802.11a WLANs. Since 802.11b and 802.11g WLANs use frequencies in the unlicensed 2.4-GHz frequency band, they are subject to several sources of interference, since many other devices also use this frequency, such as wireless phones, microwave ovens, *Bluetooth* devices, other 802.11b or 802.11g WLANs, and anything else operating in the 2.4-GHz band [33]. On the other hand, the 5-GHz band, where 802.11a systems operate, is currently much less used by other devices. Thus, interference problems are not yet a significant issue there.

However, this last advantage is not true worldwide. The *Unlicensed National Information Infrastructure* (UNII) band is relatively unpopulated in the United States, but not everywhere. In Europe, in order to permit the use of the 5-GHz band to unlicensed

applications, the *European Telecommunications Standards Institute* (ETSI) requires the use of two protocols, the *Dynamic Frequency Selection* (DFS) and the *Transmit Power Control* (TPC), that employ the dynamic changing of channels and/or use of lower power modulation, in the case of interference. In that manner, priority is given to signals already in the channel. Even worse, in Japan, only the lower 100-MHz portion of the UNII band is allowed for unlicensed use, meaning that the number of available channels goes down to five, from the eight channels that are used in the United States and Europe [5].

Among the interfering 2.4-GHz devices, wireless phones are the most harmful to the performance of the 802.11b and 802.11g WLANs. For example, the use of a cordless phone within a range of 75 feet of 802.11 devices can disrupt the operation of the WLAN [38]. The use of a microwave oven within 10 feet of 802.11b equipment will also cause a drop in its performance.

As far as Bluetooth equipment is concerned, several devices, such as laptops and PDAs, support both technologies, so they are expected to operate at the same time. Indeed, the inherent protection provided by the *Frequency Hopping Spread Spectrum* (FHSS) in Bluetooth, the *Direct Sequence Spread Spectrum* (DSSS) in the IEEE 802.11b, and the *Orthogonal Frequency Division Multiplexing* (OFDM) in the IEEE 802.11g, together with an error detecting protocol that provides for packet retransmission, may offer an acceptable performance even in cases where 802.11b or 802.11g and Bluetooth devices are used in close proximity [39]. However, in some other cases, the operation of Bluetooth devices close to 802.11b/g stations can affect the performance of the network, especially if the communicating stations are located quite far between each other. In view of this problem, the *IEEE 802.11* and *IEEE 802.15 Task Groups* are already trying to develop a new standard that will allow the coexistence of 802.11b/g and Bluetooth devices without interfering with each other.

Finally, the operation of other WLANs in the same area can also initiate interference problems, if channel selection is not properly regulated. More specifically, users located at the outer limits of the area covered by their corresponding access point may face

interference problems if another *Access Point* (AP), operated by a different provider, is close. The proper use of duplicate channels can prevent this, but the effectiveness of this solution also depends on the topology of the access sites [38].

Although 802.11b and 802.11g WLANs define eleven channels, there is a provision for devices close to each other to operate with a four–channel separation for avoiding interference. In that way, there are practically only three available channels (e.g. channels 1, 6, and 11) for every covered area. In order to prevent duplicate channels from overlapping, providers typically allocate these channels in a pattern like the one used in mobile networks, i.e., a hexagonal pattern. This scheme works satisfactorily if there is only one provider in the area, but in the case of multiple providers, they must cooperate in channel allocation to prevent interference. Unfortunately, in practice, competing network operators do not take into account interference issues as seriously as they should, often believing that they will maintain a monopoly in the area in which they operate. However, it must be realized that the continuous deployment of wireless networks everywhere will lead to proportionally increasing interference problems in the near future [38].

3. The IEEE 802.11 Standard Performance

a. Theoretical Capacities

As already mentioned, WLANs based on the IEEE 802.11b and IEEE 802.11g specifications actually provide only three non–overlapping channels, which translates to a theoretical total data rate of 33 Mbps (assuming 11 Mbps per channel) for 802.11b systems, and 162 Mbps (assuming 54 Mbps per channel) for 802.11g systems. On the other hand, since the IEEE 802.11a specification supports eight non–overlapping channels, the corresponding total data rate is 432 Mbps [38], given speeds of 54 Mbps per channel.

b. Effective Data Rates

Unfortunately, the above theoretical data rates provided by 802.11 WLANs differ largely from the actual throughputs. Indeed, the theoretical data rates of up to 11 Mbps for 802.11b networks are often about half of it in reality, sometimes even as low as 4 Mbps. The same is true for both 802.11a and 802.11g. Although they achieve data rates up to 55 Mbps in the lab, they can reach only approximately 20 Mbps in the field [40].

Although pure 802.11g WLANs offer, in practice, effective speeds of about 20 Mbps, in the case of Internet connections they provide an even lower actual throughput ranging between 10 and 20 Mbps. This significant decrease from the theoretical bit rate is due to the need of ensuring backward compatibility between new 802.11g and already existing 802.11b devices and APs. The presence of 802.11b nodes further reduces the nominal data rates of 802.11g devices, since they incorporate protection mechanisms for preventing interference with 802.11b equipment. More precisely, in mixed 802.11b and 802.11g wireless networks following the TCP/IP protocol, operating 802.11g devices transmit an electronic warning to the 802.11b devices, which results in a reduction of the true throughput down to 10 Mbps. However, speeds of 10 Mbps are not sufficient to support data–intensive applications, such as video applications, which require minimum bit rates of 20 Mbps. For these kinds of applications, providers should consider the deployment of pure 802.11g, or, even better, 802.11a WLANs, which offer an actual throughput of approximately 24 Mbps [41].

All the above actual throughputs of 802.11 WLANs may be further reduced in the presence of radio interfering signals. In the 2.4-GHz band, interference from the numerous devices using it may cause lower throughputs, which in turn, will reduce a system's effective range. On the contrary, 802.11a systems do not face significant interference in the 5-GHz band, so their actual data rates are not affected by the operation of unwanted devices [40]. It is also important to note that the effective data rates further drop when the *Wired Equivalent Privacy* (WEP) encryption mechanism is enabled, or when 802.11b and 802.11g NICs are used simultaneously in the same WEP-disabled

network. However, the attained throughputs are still higher than those of an exclusively 802.11b network. Even when 802.11b cards are connected to an 802.11g gateway, the achievable speeds increase by about 15% above the feasible ones with an 802.11b gateway [42].

c. Effective Ranges

According to early tests, 802.11g systems achieve the same, or slightly better ranges in comparison to 802.11b systems. Theoretically, both 802.11b and 802.11g are able to attain longer ranges than 802.11a, since they operate at lower frequencies. Although this is true, in practice, 802.11a systems can maintain higher speeds than 802.11b systems at comparable ranges, and better throughputs close to the limits of their covered area than 802.11g systems, which maintain much lower speeds at their limit range [40]. As the distance from the access point increases, the data rates are reduced in all specifications, but in any case 802.11a rates remain higher than those of 802.11b at similar distances. On the other hand, 802.11b systems may, indeed, reach higher ranges than 802.11a systems, but for doing so they have to decrease their rates as low as just 1 Mbps [38].

d. Resistance to Impairments

The use of OFDM in 802.11a and 802.11g systems makes them more resistant to impairments that may reduce the effective data rates, such as multipath propagation. On the contrary, 802.11b systems, which use DSSS schemes, are more susceptible to transmission impairments, since they are significantly slower [38].

D. COMPARISON BETWEEN FSO AND THE IEEE 802.11 STANDARD

1. Cost

FSO and the IEEE 802.11 standard are potentially lower–cost ways of overcoming the "last mile problem," allowing service providers to add customers quickly and easily. Both technologies turned out to be cost–effective solutions for satisfying the increasing demand for broadband services when their components became affordable, due to evolutions in optics and semiconductor technologies. Additionally, since both technologies transmit information through the atmosphere without the need to deploy fiber cables, licenses concerning digging up streets are not required. Moreover, both FSO and 802.11 systems use frequencies located in unregulated sections of the spectrum, thus no operating licenses are required. In view of the fact that there is no need to buy expensive spectrum, the cost associated with rendering a system operational is substantially reduced. However, the cost is not the same for both technologies; according to an economic analysis in [5] that provides a comparison between the deployment of an all-FSO network against an all-802.11 one, both from "scratch," for the coverage of the same area. The cost of the 802.11 solution is significantly lower than the cost of the FSO solution. Even though the analysis is based on rough estimations as many companies are hesitant about giving general cost estimations, since large variations exist depending on factors such as the specific location, the quantity of purchased equipment, the age of it, the length of the contract, etc., the cost of the very high–speed FSO link heads greatly impact the total cost of building up an FSO network, contrary to the affordable prices of APs and *Network Interface Cards* (NICs). The main drawback of an all–FSO solution is that there is no availability of small and reasonable-priced FSO link heads for home users that can provide, for example, data rates as "low" as 100 Mbps, which is the speed supported by wired Ethernet and would be more than enough for high-speed Internet. The cost of deploying an all-FSO network that would provide much higher speeds can be significantly reduced if a hybrid FSO-802.11 implementation is chosen. Given that FSO allows very high-bandwidth *trunk links*, and 802.11a or 802.11g offer good *edge links*, both FSO link

heads and 802.11 APs can be used concurrently at the network nodes, while subscribers will need to use the appropriate NICs. Of course, the cost in all cases is greatly reduced if already existing infrastructure is used [5].

Consequently, if a choice between the two technologies has to be based on cost, the IEEE 802.11 standard provides the most cost–effective solution.

2. Time of Deployment

Both FSO and 802.11 systems do not require trenches to be dug in order to lay cables, while time–consuming procedures involved with obtaining licenses for the use of the frequency spectrum are also avoided. In this manner, the installation of the required FSO or 802.11 equipment to connect a new subscriber, or even a whole neighborhood, can be completed within a few days, contrary to fiber optic systems that may require months to be deployed. Consequently, both FSO and 802.11 systems are time–attractive as well, in addition to being cost–attractive.

3. Data Rates

FSO networks support much higher data rates than 802.11 ones. Indeed, FSO systems already available on the market can achieve speeds up to 2.5 Gbps, whereas trials of systems under development have reported speeds of up to 160 Gbps. On the other hand, as previously discussed, 802.11b WLANs provide a theoretical maximum total data rate up to 33 Mbps (assuming 11 Mbps per each one of the three supported channels), and 802.11g WLANs offer maximum rates up to 162 Mbps (assuming 54 Mbps per each one of the three supported channels). The highest 802.11 capacities are provided by 802.11a WLANs with eight non–overlapping supported channels; given speeds of 54 Mbps per channel, the corresponding maximum total data rate is 432 Mbps [38]. Also, as explained earlier, these data rates are only theoretical. Effective throughputs may be much lower in practice, i.e., 5-6 Gbps for 802.11b, 10-20 Gbps for 802.11g, and 24 Gbps for 802.11a

WLANs [40]. Even these speeds may be further reduced if the WEP encryption mechanism is enabled, or if both 802.11b and 802.11g NICs are used at the same time in a WEP–disabled network.

In view of the above, FSO systems by far constitute a better choice for high–bandwidth last–mile applications.

4. Availability-Reliability

a. Influence of Weather

The transmission of information through the air must deal with the atmosphere, which is a very complex factor. As far as FSO systems are concerned, this results in unpredictable laser power attenuation. FSO links are subject to various atmospheric phenomena, i.e., *absorption*, *scattering*, and *scintillation* that contribute to signal degradation and attenuation. The extent of their impact depends on the current local weather conditions, so atmospheric attenuation is variable and difficult to predict. The impact of the weather is considered the biggest challenge in FSO communications. Although rain and snow may affect FSO systems only under very severe conditions, fog can significantly aggravate the attenuation of signals, alter the characteristics of light, or even completely obstruct the passage of light. In this manner, achievable link distances and link availability ("uptime") can be largely reduced in the presence of heavy fog. Even when using very high–powered lasers, the achievable ranges are not increased significantly, especially in very bad weather. Therefore, the particular climate conditions in the area a system is deployed may limit the availability and reliability of FSO links [23]. Due to the weather–related issues, FSO systems cannot achieve 100% availability. The outages that can be tolerated in a specific application determine if the corresponding availability, and, thus, the reliability of a FSO system, is acceptable or not.

Mie scattering, the responsible process for the fog influence in open–air optical transmissions, is not an issue in RF communications. On the other hand, *Rayleigh scattering* due to rain, which does not seriously affect FSO wavelengths, causes signal fading and attenuation at radio wavelengths, in a similar way to the effect of fog in FSO communications. RF wireless technologies using frequencies above approximately 10 GHz are not notably affected by fog, but they are significantly affected by rain, since the RF wavelengths are close to the radius of raindrops, both being larger than the fog droplets. In that way, high-frequency radio signals with wavelengths in the millimeter to centimeter range are susceptible to rain fading caused by Rayleigh scattering [20]. Nevertheless, the lower RF frequencies in the 2.4-GHz and 5-GHz bands that are used in 802.11 systems are relatively unaffected by both rain and fog. For this reason, the impact of the weather is not an important issue to consider in the deployment of 802.11 networks.

According to the above, 802.11 WLANs are better, in terms of availability and reliability, than FSO WLANs in areas where unfavorable weather conditions are common.

b. Physical Obstructions

If the line–of–sight requirement is not met, the operation of a FSO link will be disrupted, since light cannot pass through solid objects. Due to the narrow beams used and the high data rates, even small obstacles can interrupt FSO communications. Therefore, unobstructed line–of–sight between transmitters and corresponding receivers is a strict requirement for FSO systems. Even though this requirement is not as rigorous as in 802.11 systems, physical obstacles in the path of radio signals can result in adverse phenomena such as *path loss* and *multipath effect*, which may cause the attenuation (or *multipath loss*), the distortion, or even the total cancellation of a sent signal, as explained in the previous chapter. Although the 802.11 technology has generally proved reliable in transferring information over long distances, the large variability in the environments where 802.11 systems operate makes the estimation of the maximum coverage ranges difficult [29]. The distances over which radio waves can reliably transfer information in

802.11 WLANs depend on the objects that signals encounter on route, as well as on the specific materials these objects are made of, because some radio frequencies can penetrate some materials, while others not. In view of this fact, the existence of line–of–sight is also desired, although not obligatory, in 802.11 networks. In any case, the 802.11 operation is more reliable in the presence of various objects over the communication path than the FSO operation.

c. Building Movements

Another significant factor to consider in the installation of FSO systems is the natural building movements that affect beam aiming. If the beam divergence is less than the sway of the building where the intended receiver is installed, the beam may be totally mispointed, and miss its target. The exact beam pointing is very important, since even a slight misalignment between the receiver and the transmitter can cause signal losses, or the total interruption of a communication link [16]. Of course, this is not a problem in 802.11, where radio signals are transmitted over much wider angles.

d. Radio Interference

The free use of unlicensed parts of the frequency spectrum often means serious interference problems associated with these frequencies. As discussed earlier, several popular devices use the 2.4-GHz band, where 802.11b and 802.11g systems also operate. These represent severe interference sources that may reduce even further the effective data rates and ranges. On the other hand, 802.11a systems do not encounter substantial interference by the few devices using the 5-GHz band, so 802.11a WLANs enjoy a higher degree of availability. This is the present situation, which may change in the future. Additionally, interference caused by different wireless networks operating near each other is becoming more and more a significant issue with the increasing installation of WLANs in every possible area.

Contrarily, FSO operation does not encounter interference problems, due to the use of very narrow highly directional light beams. In this respect, FSO systems are much more reliable, based on interference criteria, especially in areas where pre-installation surveys indicate the presence of numerous interfering sources.

5. Security

Security issues in wireless networking are associated with transferring data through the open air, without physical constraints. Due to their own nature, wireless communications are by default vulnerable to interceptions. In fact, security problems are very common in radio frequency, or microwave–based communication systems, where typical antennas interconnecting two remote sites in a point–to–point link spread the radiation over angles between 5 and 25 degrees. The wide spreading of the beam, in combination with the operation of the microwave antennas at very high power levels, is the main reason for the security worries. These problems were not realized early enough. Thus, the security mechanisms currently provided by the IEEE 802.11 standard have many vulnerabilities and security holes, and may not provide the desired protection against eavesdropping.

On the other hand, interception in FSO systems is extremely difficult, thanks to the use of very narrow beams, usually much less than 8.727 milliradians (0.5 degrees), and the limited length of the optical links. Moreover, the fact that beams are typically transmitted at a significant height renders their potential interception even more difficult.

Consequently, FSO communication systems are among the most secure networking transmission technologies, their interception being far more difficult, compared to RF or microwave communication systems. Unlike microwave systems, it is extremely difficult to intercept the FSO light beam carrying networking data, because the information is not spread out in space, but rather kept in a very narrow cone of light. In respect to this, if security is the major concern in the operation of a wireless network whose development is under consideration, the use of FSO technology is clearly the best solution.

All the above comparisons between FSO and 802.11 technologies are summarized in the following table.

	FSO	**802.11**
DEPLOYMENT COST	Lower than fiber, but still higher than 802.11	Low
DEPLOYMENT TIME	Very low	Very low
DATA RATES	Very high	High
WEATHER	Significant impact	Low impact
PHYSICAL OBSTRUCTIONS	Interruption of the communication link	Can be a problem, but less than with FSO
BUILDINGS MOVEMENTS	Important impact	No impact
INTERFERENCE	No impact	Important impact in the 2.4-GHz band, still low impact in the 5-GHz band
SECURITY	Very high	Low

Table 4. Comparing the Strengths and Weaknesses of FSO and 802.11 Technologies.

E. SUMMARY

This chapter discussed the advantages and limitations of both FSO and IEEE 802.11 WLAN technologies when implemented in the "last mile," and provided a comparison among them in the sectors of the greatest interest.

VI. CONCLUSIONS

The “last mile problem” is one of the most significant issues in the communications sector, since existing copper wire infrastructure cannot provide the essential bandwidth for today’s bandwidth–intense applications, and currently available wired access technologies have proven unable to address the increasing demands for larger bandwidth and provide an adequate high–speed solution. Fiber–optics technology has the capability to fulfill the demands for higher data rates and more bandwidth, but the cost and time associated with obtaining licenses to dig trenches and install fiber optic cables, as well as the cost of operation and maintenance, are prohibitive factors to the adoption of the technology on a larger scale. Although not discussed in this thesis, political and regulatory obstacles have also been a major factor in the United States [43]. Even when fiber cables are installed, future upgrade and scalability needs will once again have to address the problems of high cost and time resources. Under these circumstances, homes and offices in the “last mile” request the same access speeds that are available in the fiber backbone, but their desires are not satisfied, since providers are unwilling to undertake the cost and the associated risk of bringing new fiber optic cables to every home and business. Thus, new ways for reaching “last mile” homes and businesses and offering them access to a high-speed network have to be explored.

Within this context, several wireless suggestions have been made. New wireless broadband technologies are becoming more and more attractive, since they are technically and economically feasible solutions for bringing high–speed network access to individual neighborhoods, and can service different customers in a price hierarchy, in order to provide affordable bandwidth to everyone. Thus, wireless approaches are not only among the candidates to solve the “last mile problem,” but seem to be quite promising for supporting broadband services in homes and businesses not connected to the fiber backbone. The main benefits of wireless versus wired technologies are their performance in terms of bandwidth, their lower deployment cost, simpler and faster installation, and their inherent flexibility that supports scalability and demand–based build out.

This thesis studied two wireless technologies for their potential in solving the "last mile problem": *Free Space Optics* (FSO) and the *IEEE 802.11 Wireless Local Area Networking* (WLAN) standard. Initially, the network access problems associated with the existing wired connections in homes and businesses in the "last mile" were discussed. Then, an analysis of both FSO and the IEEE 802.11 WLAN standard was provided, discussing their theoretical background, and emphasizing the technological aspects upon which they are based, as well as performance and propagation issues. This thesis identified and determined their strengths and weaknesses, in general, and as solutions in the "last mile," in particular. Finally, the thesis presented a comparison between the two technologies as potential candidates to solve the "last mile problem."

FSO technology provides very high–speed network access, fast deployment, very high levels of security, and lower cost than fiber systems. However, it is still expensive for home and small–office users. Furthermore, weather and atmospheric conditions can adversely affect FSO operation, resulting in support of true high-bandwidth capability only over relatively limited link lengths. FSO networks also strictly require line–of–sight links and sufficiently precise beam pointing.

On the other hand, the cost involved with developing an IEEE 802.11 WLAN network is significantly lower than the cost associated with deploying either fiber or FSO systems. The time of deployment is also low, the impact of the weather conditions is less critical, the line–of–sight requirement is less strict than in FSO networks, and precise pointing is not an issue. However, the disadvantages of the technology, in comparison to FSO, are the lower data rates, interference problems caused by other neighboring radio devices or WLANs, multipath–related issues in the presence of physical obstructions, and insufficient degree of security.

One result from the research is the realization that a single answer does not exist to the question of which is the most appropriate to solve the "last mile problem." The decision has to be case–specific, depending on numerous factors. Thus, several other issues have to be considered:

- What cost is affordable?
- What data rates are needed for the intended applications?
- What degree of security is needed?
- How critical is the data to be transmitted? How reliable must the system be?
- What physical obstructions exist in the area where the system will be installed?
- How heavy is interference in the location of installation?
- What are the particular climate conditions in the region? How much can weather–related outages be tolerated?

Different areas and locations vary greatly. Thus, different solutions may be more appropriate for different sites. For example, if the presence of heavy fog is common in an area, installing a FSO network is not the best solution. The “best” technology for one area may not be best for another. Before a decision is made, a detailed site–specific survey must be performed. Once the benefits and drawbacks, concerning the implementation of each proposed solution in the area of interest, are determined and compared, a better choice can be made.

Apart from the two technologies discussed in this thesis, there are other “last mile” technologies as well. The existence of more alternatives will drive the competition between them and better solutions will arise. Therefore, other alternatives should also be studied and compared to those of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. *Intel Processor History,* Intel, [http://www.intel.com/intel/intelis/museum/exhibits/hist_micro/], last accessed August 2003.
2. John W. Sprague, "Free space optics and wireless broadband radio frequency technology: bringing high-speed network access to the last mile," Master's Thesis, Naval Postgraduate School, Monterey, California, March 2002.
3. LightPointe Communications Inc., [http://www.freespaceoptics.org/index.cfm/fuseaction/content.FAQs], last accessed August 2003.
4. Heinz Willebrand and Baksheesh S. Ghuman, "Introduction to free-space optics," *Free-Space Optics: Enabling Optical Connectivity in Today's Networks*, pp. 2-7, Sams Publishing, Indianapolis, 2002.
5. Peng Joo Lee, "Alternate high speed network access for the last mile," Master's Thesis, Naval Postgraduate School, Monterey, California, December 2002.
6. Heinz Willebrand and Baksheesh S. Ghuman, "Fundamentals of FSO technology," *Free-Space Optics: Enabling Optical Connectivity in Today's Networks,* pp. 10-46, Sams Publishing, Indianapolis, 2002.
7. Michael Kenward, *Laser Technology Sheds Light on Connection Issue (The Financial Times*, 7-16-2001), fSONA, [http://www.fsona.com/company.php?sec=press_financialtimes], last accessed August 2003.
8. *Lighting Up the Last Mile with Optics,* NetworkWorldFusion, [http://www.nwfusion.com/news/tech/2002/0722tech.html], last accessed August 2003.
9. *FSO Technology,* LightPointe Communications Inc., [http://www.lightpointe.com/index.cfm?fuseaction=news.NewsArchives], last accessed August 2003.
10. *History of Free Space Optics (FSO),* LightPointe Communications Inc., [http://www.free-space-optics.org/], last accessed August 2003.
11. *A Brief History of FSO,* Shorecliff Communications LLC, [http://www.shorecliffcommunications.com], last accessed August 2003.
12. O. Ozkok and O. Timus, Class project for CS4554 (Free Space Optics), Naval Postgraduate School, 2003 (unpublished).
13. AirFiber Inc., [http://www.airfiber.com/index.shtml], last accessed August 2003.
14. Heinz Willebrand and Baksheesh S. Ghuman, "Fiber Optics without Fiber," *IEEE Spectrum,* Vol. 38, Issue 8, pp. 40-45, August 2001.

15. *Free-Space Optics: A Viable Last Mile Alternative*, LightPointe Communications Inc., [http://www.freespaceoptics.org/index.cfm/fuseaction/content.WhitePapers], last accessed August 2003.

16. Leonidas Fountanas, "An assessment of emerging wireless broadband technologies," Master's Thesis, Naval Postgraduate School, Monterey, California, December 2001.

17. Heinz Willebrand and Baksheesh S. Ghuman, "Factors affecting FSO," *Free-Space Optics: Enabling Optical Connectivity in Today's Networks*, pp. 48-60, Sams Publishing, Indianapolis, 2002.

18. Soo Sim Daniel Neo, "Free Space Optics communication for mobile military platforms," Master's Thesis, Naval Postgraduate School, Monterey, California, December 2003.

19. *FSO Challenges*, LightPointe Communications Inc., [http://www.freespaceoptics.org/index.cfm/fuseaction/content], last accessed August 2003.

20. Daniel Chu, *Free-space Optics Leaps Last Mile*, 15 April 2002, EE TIMES, [http://www.eetimes.com/in_focus/communications/OEG20020412S0066], last accessed August 2003.

21. *Free-Space Optics: Transmission Security*, 2002, LightPointe Communications Inc., [http://www.freespaceoptics.org/index.cfm/fuseaction/content.WhitePapers], last accessed August 2003.

22. Heinz Willebrand, *Free Space Optics*, Internet Industry Magazine, [http://www.internetindustry.com/mag/01_02su/09fre/], August 2003.

23. *Free Space Optics (FSO) Challenges*, Free Space Optics, [http://www.free-space-optics.org/index.php], last accessed August 2003.

24. James LaRocca and Ruth LaRocca, "802.11 – Bridging the gap," *802.11 Demystified*, pp. 5-11, McGraw-Hill, New York, 2002.

25. Hamed Almantheri, "Computer wireless networks: a designed plan for building wireless networks using IEEE 802.11 standard," Master's Thesis, Naval Postgraduate School, Monterey, California, March 2003.

26. James LaRocca and Ruth LaRocca, "The IEEE 802.11 alphabet spelled out," *802.11 Demystified*, pp. 18-30, McGraw-Hill, New York, 2002.

27. Theodore S. Rappaport, "Mobile radio propagation: small-scale fading and multipath," *Wireless Communications Principles and Practice*, pp. 177-178, Prentice Hall, Upper Saddle River, New Jersey, 2002.

28. Steve Kapp, *802.11: Leaving the Wire Behind*, IEEE Internet Computing, [http://csdl.computer.org/comp/mags/ic/2002/01/w1082abs.htm], last accessed August 2003.

29. James LaRocca and Ruth LaRocca, "Physical concepts and architecture," *802.11 Demystified*, pp. 122-131, McGraw-Hill, New York, 2002.

30. William Stallings, “Spread spectrum,” *Wireless Communications and Networks*, pp. 168-176, Prentice Hall, Upper Saddle River, New Jersey, 2002.

31. William Stallings, “Data encoding,” *Data and Computer Communications*, pp. 162-166, Prentice Hall, Upper Saddle River, New Jersey, 2000.

32. William Stallings, “High-speed LANs,” *High-Speed Networks and Internets: Performance and Quality of Service*, pp. 124-126, Prentice Hall, Upper Saddle River, New Jersey, 2002.

33. James LaRocca and Ruth LaRocca, “Implementation,” *802.11 Demystified*, pp. 177-185, McGraw-Hill, New York, 2002.

34. William Stallings, “IEEE 802.11 wireless LAN standard,” *Wireless Communications and Networks*, pp. 458-477, Prentice Hall, Upper Saddle River, New Jersey, 2002.

35. *WLAN Connectivity with Free-Space Optics*, 2002, LightPointe Communications Inc., [http://www.lightpointe.com/index.cfm?fuseaction=tecnology.WhitePapers], last accessed August 2003.

36. James LaRocca and Ruth LaRocca, “Wireless LAN (WLAN) security,” *802.11 Demystified*, pp. 144-150, McGraw-Hill, New York, 2002.

37. *Link Range – How Far will FSO Work?*, Free Space Optics (FSO) – Information Website for Gigabit Wireless, [http://www.freespaceoptics.com/Free_Space_Optics_Link_Range.html], last accessed August 2003.

38. Jim Geier, *802.11a Becomes a Contender*, 17 June 2002, Network World, [http://www.nwfusion.com/reviews/2002/0617bg1.html], last accessed February 2004.

39. Terry Bourk, *Techniques Mitigate Interference Between 802.11 and Bluetooth*, 8 November 2002, EE TIMES, [http://www.eetimes.com/in_focus/mixed_signals/OEG20021107S0022], last accessed February 2004.

40. Steven J. Vaughan-Nichols, *802.11g: The Next Big Thing or the Next Last Thing*, 30 September 2002, Internetnews, [http://siliconvalley.internet.com/news/article.php/1472641], last accessed February 2004.

41. Bob Brewin, *Final 802.11g Standard Throttles Data Rates Down*, 22 May 2003, InfoWorld, [http://www.infoworld.com/article/03/05/22/HNwirestandard_1.html], last accessed February 2004.

42. Becky Waring, *Best Wi-Fi Ever: 802.11g* (PC World magazine, April 2003), PC World, [http://www.pcworld.com/news/article/0,aid,109583,00.asp], last accessed February 2004.

43. Federal Communications Commission, [http://www.fcc.gov/], last accessed February 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Chairman Code CS
   Department of Computer Science
   Naval Postgraduate School
   Monterey, California

4. Chairman Code EC
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

5. Professor Gilbert M. Lundy
   Naval Postgraduate School
   Monterey, California

6. Professor Roberto Cristi
   Naval Postgraduate School
   Monterey, California

7. Antonios Varelas
   Lieutenant Commander, Hellenic Navy
   Athens, Greece